

501.39836X00

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): S. AKAHANE ET AL.

Serial No.: Not Yet Assigned

Filed: March 20, 2001

For: VPN ROUTER AND VPN ROUTER IDENTIFICATION METHOD
BY USING LOGICAL CHANNEL IDENTIFIERS



CLAIM FOR PRIORITY

Assistant Commissioner for Patents
Washington, D.C. 20231

March 20, 2001

Sir:

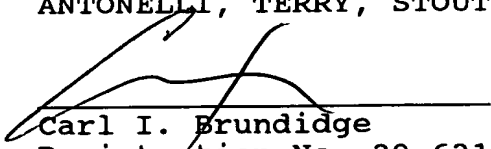
Under the provisions of 35 U.S.C. and 37 CFR 1.55, the
applicants hereby claim the right of priority based on:

Japan 2000-170414, filed June 2, 2000

The certified copy of said Japanese application is
attached hereto.

Respectfully submitted,

ANTONELLI, TERRY, STOUT & KRAUS


Carl I. Brundidge
Registration No. 29,621

CIB:alw
(703) 312-6600

日 本 国 特 許 庁

PATENT OFFICE
JAPANESE GOVERNMENT

JCS71 U.S. PTO
09/811440



別紙添付の書類に記載されている事項は下記の出願書類に記載されて
る事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
with this Office.

出 願 年 月 日
Date of Application:

2000年 6月 2日

願 番 号
Application Number:

特願2000-170414

願 人
Applicant(s):

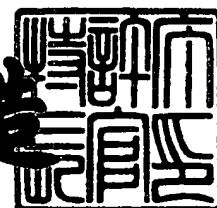
株式会社日立製作所

CERTIFIED COPY OF
PRIORITY DOCUMENT

2000年10月 6日

特許庁長官
Commissioner,
Patent Office

及 川 耕 造



【書類名】 特許願

【整理番号】 H00010411A

【提出日】 平成12年 6月 2日

【あて先】 特許庁長官 殿

【国際特許分類】 H04L 12/56

【発明者】

 【住所又は居所】 東京都国分寺市東恋ヶ窪一丁目 2 8 0 番地
 株式会社日立製作所中央研究所内

 【氏名】 赤羽 真一

【発明者】

 【住所又は居所】 東京都国分寺市東恋ヶ窪一丁目 2 8 0 番地
 株式会社日立製作所中央研究所内

 【氏名】 坂本 健一

【発明者】

 【住所又は居所】 神奈川県秦野市堀山下 1 番地
 株式会社日立製作所エンタープライズサーバ事業部内

 【氏名】 須貝 和雄

【特許出願人】

 【識別番号】 000005108

 【氏名又は名称】 株式会社日立製作所

【代理人】

 【識別番号】 100075096

 【弁理士】

 【氏名又は名称】 作田 康夫

 【電話番号】 03-3212-1111

【手数料の表示】

 【予納台帳番号】 013088

 【納付金額】 21,000円

【提出物件の目録】

【物件名】	明細書	1
【物件名】	図面	1
【物件名】	要約書	1
【プルーフの要否】	要	

【書類名】 明細書

【発明の名称】 ルータ装置、パケット転送制御方法及びVPN識別情報の設定方法

【特許請求の範囲】

【請求項 1】

複数のバーチャル・プライベート・ネットワーク（以下、「VPN」という。）を収容することができるルータ装置であって、

複数の論理チャネルが多重された受信回線を収容する物理インタフェースと、

上記複数の論理チャネルの各論理的なチャネルに割り当てられている論理チャネル識別子と、上記複数のVPNに割り当てられているVPN名との対応関係を示すテーブルを保持するメモリと、

上記複数の論理チャネルのうちの一つの論理チャネルを介して送信されたパケットを受信した際、上記論理チャネルに割り当てられている論理チャネル識別子を検索キーとして上記テーブルを検索し、上記受信パケットが上記複数のVPNのうち何れのVPNに属するかを判断する処理部、とを有することを特徴とするルータ装置。

【請求項 2】

請求項 1 に記載のルータ装置であって、

それぞれ、送信回線が収容される複数の物理インタフェースと、

上記複数のVPNの各VPN対応に、各VPNで使用されるパケットのアドレス情報と、上記複数の物理インタフェースを識別する情報との対応関係を示すルーティングテーブルを保持するメモリ、とを有し、

上記処理部は、上記パケットのヘッダ部に格納される宛先アドレス情報を検索キーとして上記ルーティングテーブルを検索し、上記複数の物理インタフェースのうち何れの物理インタフェースから上記受信パケットを送信するかを決定することを特徴とするルータ装置。

【請求項 3】

請求項 2 に記載のルータ装置であって、

上記ルーティングテーブルは、各VPNで使用されるパケットのアドレス情報と、パケットを出力する際に付与するヘッダ情報との関係を保持し、

上記処理部は、上記パケットのヘッダ部に格納される宛先アドレス情報を検索キーとして上記ルーティングテーブルを検索し、上記受信パケットに付与するパケットヘッダ情報を決定することを特徴とするルータ装置。

【請求項4】

請求項2又は請求項3の何れかに記載のルータ装置であって、

上記テーブルと上記ルーティングテーブルとは物理的に同一のメモリ上に保持されることを特徴とするルータ装置。

【請求項5】

請求項1乃至請求項4の何れかに記載のルータ装置であって、

上記受信回線は、非同期転送モード(ATM)回線であり、上記論理チャネル識別子は、VPI及びVCIであることを特徴とするルータ装置。

【請求項6】

請求項1乃至請求項4の何れかに記載のルータ装置であって、

上記受信回線は、フレームリレー回線であり、上記論理チャネル識別子は、LCIであることを特徴とするルータ装置。

【請求項7】

請求項1乃至請求項4の何れかに記載のルータ装置であって、

上記受信回線は、L2TP(Layer2 Tunneling Protocol)で規定されているL2TPヘッダでカプセル化されたパケットが送信され、上記論理チャネル識別子は、L2TPカプセルヘッダ内の情報であることを特徴とするルータ装置。

【請求項8】

請求項1乃至請求項4の何れかに記載のルータ装置であって、

上記受信回線は、イーサネット回線であり、上記論理チャネル識別子は、IEEE 802.1Qで規定されるVLAN Tagであることを特徴とするルータ装置。

【請求項9】

請求項1乃至請求項4の何れかに記載のルータ装置であって、

上記受信回線は、PPP Over Ethernetでカプセル化されたパケットが送信され

、上記論理チャネル識別子は、そのカプセルヘッダ内の情報であることを特徴とするルータ装置。

【請求項 1 0】

請求項 1 乃至請求項 9 の何れかに記載のルータ装置であって、

上記ルータ装置は、制御端末と接続することが可能であり、

上記制御端末から、上記テーブル内に保持される上記論理チャネル識別子と、上記 V P N 名との対応関係を設定することができることを特徴とするルータ装置

【請求項 1 1】

ルータ装置であって、

第 1 のバーチャル・プライベート・ネットワーク（以下、「V P N」という。）に属する第 1 のローカル・エリア・ネットワーク（以下「L A N」という。）及び第 2 の V P N に属する第 2 の L A N から同一のプロトコルでカプセル化されたパケットが多重されて送信される回線を収容するインタフェース部と、

上記第 1 の回線から受信したパケットが上記第 1 の V P N に属するのか、上記第 2 の V P N に属するのかを識別するための識別子を設定する手段、

とを有することを特徴とするルータ装置。

【請求項 1 2】

請求項 1 1 に記載のルータ装置であって、

上記プロトコルは非同期転送モードプロトコルであり、上記識別子は V P I 及び V C I であることを特徴とするルータ装置。

【請求項 1 3】

ルータ装置であって、

それぞれ、異なるバーチャル・プライベート・ネットワーク（以下、「V P N」という。）に属する複数のローカル・エリア・ネットワーク（以下「L A N」という。）から第 1 のプロトコルでカプセル化されたパケットが送信される第 1 の回線を収容する第 1 のインタフェース部と、

それぞれ、異なる V P N に属する V P N に属する複数の L A N から第 2 のプロトコルでカプセル化されたパケットが送信される第 2 の回線を収容する第 2 のイ

インタフェース部と、

上記第 1 の回線から受信したパケットが何れの VPN に属するのかを識別するための第 1 の識別子を設定する手段と、

上記第 2 の回線から受信したパケットが何れの VPN に属するのかを識別するための第 2 の識別子を設定する手段とを有し、

上記第 2 の識別子は上記第 1 の識別子とは異なることを特徴とするルータ装置

【請求項 1 4】

請求項 1 3 に記載のルータ装置であって、

上記第 1 のプロトコルは非同期転送モードプロトコルであり、上記第 1 の識別子は V P I 及び V C I であり、

上記第 2 のプロトコルはフレームリレーであり、上記第 2 の識別子は D L C I であることを特徴とするルータ装置。

【請求項 1 5】

ルータ装置であって、

第 1 のバーチャル・プライベート・ネットワーク（以下、「VPN」という。）に属する第 1 のローカル・エリア・ネットワーク（以下「LAN」という。）から第 1 のプロトコルでカプセル化されたパケットと、第 2 の VPN に属する第 2 の LAN から上記第 1 のプロトコルでカプセル化されたパケットとが多重されて送信される第 1 の回線を収容する第 1 のインタフェース部と、

第 3 の VPN に属する第 3 の LAN から第 2 のプロトコルでカプセル化されたパケットが送信される第 2 の回線と、第 4 の VPN に属する第 4 の LAN から上記第 2 のプロトコルでカプセル化されたパケットが送信される第 3 の回線とを収容する第 2 のインタフェース部と、

上記第 1 の回線から受信したパケットが上記第 1 の VPN に属するのか、上記第 2 の VPN に属するのかを識別するための第 1 の識別子を設定する手段と、

上記第 2 の回線及び上記第 3 の回線から受信したパケットが上記第 3 の VPN に属するのか、上記第 4 の VPN に属するのかを識別するための第 2 の識別子を設定する手段、

とを有し、

上記第 2 の識別子は上記第 1 の識別子とは異なることを特徴とするルータ装置

【請求項 1 6】

請求項 1 5 に記載のルータ装置であって、

上記第 1 のプロトコルは非同期転送モードプロトコルであり、上記第 1 の識別子は V P I 及び V C I であり、

上記第 2 のプロトコルは P P P over S O N E T であり、上記第 2 の識別子は、上記第 3 の回線と上記第 4 の回線とを識別するための物理インタフェース番号であることを特徴とするルータ装置。

【請求項 1 7】

複数のバーチャル・プライベート・ネットワーク（以下、「VPN」という。）を収容することができるルータ装置におけるパケット転送制御方法であって、

上記ルータ装置は、複数の論理チャネルが多重された受信回線を収容し、上記複数の論理チャネルの各論理的なチャネルに割り当てられている論理チャネル識別子と、上記複数の VPN に割り当てられている VPN 名との対応関係を示すテーブルを有し、

上記方法は、

上記複数の論理チャネルのうちの一つの論理チャネルを介して送信されたパケットを受信し、

上記論理チャネルに割り当てられている論理チャネル識別子を検索キーとして上記テーブルを検索し、

上記受信パケットが上記複数の VPN のうち何れの VPN に属するかを判断する、ステップを有することを特徴とする。

【請求項 1 8】

請求項 1 7 に記載のパケット転送制御方法であって、

上記受信回線は、非同期転送モード（A T M）回線であり、上記論理チャネル識別子は、V P I 及び V C I であることを特徴とするパケット転送制御方法。

【請求項 1 9】

それぞれ異なるバーチャル・プライベート・ネットワーク（以下、「VPN」という。）に属する複数のローカル・エリア・ネットワーク（LAN）を収容するルータ装置におけるVPN識別情報の設定方法であって、

上記ルータ装置は、上記複数のLANの一部のLANからは第1のプロトコルでカプセル化されたパケットを受信し、上記複数のLANの他のLANからは第2のプロトコルでカプセル化されたパケットを受信し、そして、メモリを有し、
上記方法は、

上記一部のLANから受信したパケットが何れのVPNに属するのかを識別するための第1の識別子を上記メモリに設定し、

上記他のLANから受信したパケットが何れのVPNに属するのかを識別するための第2の識別子を上記メモリに設定し、

上記第2の識別子は上記第1の識別子とは異なることを特徴とする。

【請求項 2 0】

請求項 1 9 に記載のVPN識別情報の設定方法であって、

上記第1の識別子と、VPNに割り当てられているVPN番号との対応関係を示す第1のテーブルを設定し、

上記第2の識別子と、VPNに割り当てられているVPN番号との対応関係を示す第2のテーブルを設定する、

ステップを更に有することを特徴とするVPN識別情報の設定方法。

【請求項 2 1】

請求項 1 9 又は請求項 2 0 の何れかに記載のVPN識別情報の設定方法であって、

上記第1のプロトコルは非同期転送モードプロトコルであり、上記第1の識別子はVPI及びVCIであり、

上記第2のプロトコルはフレームリレーであり、上記第2の識別子はDLCIであることを特徴とするVPN識別情報の設定方法。

【請求項 2 2】

複数のバーチャル・プライベート・ネットワーク（以下、「VPN」という。）

) を

収容するルータ装置におけるパケット転送制御方法であって、

レイヤ 2 に相当するプロトコルによるカプセルヘッダが付与された I P パケットを受信し、

上記カプセルヘッダ内の情報を用いて、上記受信した I P パケットが何れの V P N に属するかを決定する、

ステップを有することを特徴とするパケット転送制御方法。

【請求項 2 3】

複数のバーチャル・プライベート・ネットワーク（以下、「V P N」という。

) を収容するルータ装置であって、

レイヤ 2 に相当するプロトコルによるカプセルヘッダが付与された I P パケットを受信するインタフェース部と、

上記カプセルヘッダ内の情報を用いて、上記受信した I P パケットが何れの V P N に属するかを決定する手段、

とを有することを特徴とするルータ装置。

【発明の詳細な説明】

【 0 0 0 1】

【発明の属する技術分野】

本発明はルータ装置、そのパケット転送制御方法及びルータ装置内のルーティング情報設定方法に係り、特にインターネットにおける仮想専用網（V P N : Virtual Private Network）を構築するルータ装置、その転送制御方法、その設定方法に関する。

【 0 0 0 2】

【従来の技術】

従来、異なる地域に存在する複数の企業内網をネットワークにより接続する場合、企業は企業内網を専用線で相互接続することによって、外部のネットワークから隔絶した（つまりセキュリティが確保された）ネットワークを構築していた。しかし、専用線を使用するとネットワークコストが上昇してしまうという問題があった。このため、廉価で使用できるインターネットの普及に伴い、インター

ネットを利用して低コストの仮想的な専用線網（以下、VPN: Virtual Private Networkと呼ぶ）を構築する技術に対する要求が高まってきた。この技術は、IP (Internet Protocol) ネットワークが提供するIPあるいはIPの下位レイヤの機能を用いて、専用網を仮想的にインターネット上に構築するものである。この技術により、IPネットワーク上でも、外部のネットワークから隔絶された安全でかつ何らかの品質保証が行えるネットワークを構築することができる。

【0003】

VPNを実現する方式としては、VPNを提供するインターネットサービスプロバイダ（以下、ISPと呼ぶ）のネットワークの入り口でカプセル化を行い、ISPのネットワーク上ではこのカプセル化したヘッダに基づき転送を行い、ネットワークの出口でカプセルヘッダをはずす方式により転送を行う方式がある。インターネットの内部ではVPN固有のカプセル化ヘッダを用いることにより、セキュリティの確保されたVPNを構成することが出来る。このカプセル化の具体的なプロトコルとしては、IPカプセル化、MPOA (Multi Protocol Over ATM)、MPLS (Multi Protocol Label Switching) 等の方式があり、2000年5月現在、IETFなどの標準化団体で標準化が進められている。

【0004】

【発明が解決しようとする課題】

IPアドレスには、グローバルIPアドレスと、プライベートIPアドレスとがある。グローバルIPアドレスは世界的に一意に定められるものであるのに対し、プライベートIPアドレスは企業が自由に定めることができるものである。企業内網では、プライベートIPアドレスが用いられる場合が多い。したがって、企業がVPNサービスを利用する場合においても、プライベートIPアドレスを使用することが望ましい。この場合、複数のVPN間で同一のIPアドレスが使用される可能性がある。複数のVPN間のIPアドレスがバッティングする場合、それぞれのVPNのパケットを正しく処理するため、ISPネットワークの入り口に位置し、かつ、VPNに属するLAN (Local Area Network) を収容するルータ（以下、VPNエッジルータと呼ぶ）は、VPN毎のルーティングテ

ーブルを保持する必要がある。VPNエッジルータは、パケットを受信すると、そのパケットがどのVPNに属するLANからのパケットかを判定する。その後、VPNエッジルータは、当該VPN用のルーティングテーブルを検索してISP内ネットワークでの転送先の決定、およびカプセル化を行う。VPNエッジルータはVPN毎にルーティングテーブルを保持しているので、VPNエッジルータは、異なるVPNから受信した同一の宛先IPアドレスを持つパケットを混同せず、正しく転送することができる。

【0005】

前記VPNを識別する方式としては、例えば「日経コミュニケーション」、1999年10月18日号、p. 100、に記載されているように、ユーザ回線インターフェース単位に、VPNを一意に識別するためのVPN-IDを割り当て、このVPN-IDによりVPN識別を行う方式がある。すなわち、VPNの識別単位は物理インターフェース毎ということになる。この場合、物理インターフェース一つがVPN一つに対応している必要がある。

【0006】

しかし前記の方式では、企業ネットワークからISPネットワークまでが、一つの物理回線で接続されている必要がある。また、一つの企業ネットワークを複数のVPNと接続させたい場合、そのVPNの数だけ物理回線を用意する必要がある。さらに、VPNエッジルータは、収容するVPNの数だけ物理インターフェースを保持する必要がある。このため、VPNエッジルータが収容するVPNの数が大きくなると、VPNエッジルータの物理インターフェース数及びルータ自体の数も大きくなるという問題がある。

【0007】

企業ネットワークからVPNサービスを行うISPネットワークまでのアクセス手段として、別のISPあるいはキャリアが提供するATM網やフレーム・リレー等を用いる場合、ISPの入り口では1つの物理インターフェース内に複数の論理的なチャネルが多重されているため、物理インターフェースでVPN識別を行うことはできないという問題もある。

【0008】

本発明の目的は、物理インターフェースに多重化されている論理的なチャンネル番号を用いてVPN識別を可能にすることである。

【0009】

また、本発明の他の目的は、ルータがLANを収容する際、IPの下位レイヤとして複数の異なるプロトコルを用いる場合でも、それぞれのプロトコルに対応した適切なVPN識別情報を用いてVPN識別を行うことを可能にすることである。

【0010】

【課題を解決するための手段】

前記課題を解決するため、本発明のVPNエッジルータは、物理インターフェースに多重化されている論理的なチャンネルを識別するためのチャンネル番号を用いてVPNを識別する。論理的なチャンネル番号として、IPの下位レイヤの情報、例えば、OSIモデルで規定されているレイヤ2に相当する情報を用いる。論理的なチャンネル番号の例をいくつか挙げると、IPパケットの下位レイヤがATMの場合は、VPI、VCI等のヘッダ情報を、下位レイヤがフレームリレーの場合はDLCIを論理的なチャンネル番号として用いることができる。また、IPパケットがL2TP (Layer2 Tunneling Protocol) で規定されているL2TPヘッダでカプセル化されている場合には、L2TPカプセルヘッダ内の情報（トンネルID、セッションID等）を論理的なチャンネル番号として用いることができる。下位レイヤがイーサネット、IEEE802.1Qで規定されるVLAN Tagを用いてVPNの識別が行われる場合、前記論理的なチャンネル番号としてVLAN Tagを用いることができる。IPパケットがPPP Over Ethernetカプセル化方式で規定されているカプセル情報でカプセル化されている場合には、PPP Over Ethernetカプセル化方式で規定されているカプセル情報（セッションID等）を論理的なチャンネル番号として用いることができる。

【0011】

さらに、VPNエッジルータに、VPN識別に用いる識別子を設定するためのVPN識別子設定テーブルを設ける。この設定をVPNエッジルータを管理する

I S P の管理者が行えるようにするため、V P N エッジルータにユーザインターフェースを設ける。I P の下位レイヤが A T M の場合を例に説明すると、V P N 識別を物理インターフェースで行う場合には、前記 V P N 識別子設定テーブルに物理インターフェースと設定する。また、V P N 識別を V P I、V C I で行う場合には、前記 V P N 識別子設定テーブルに V P I、V C I と設定する。

【 0 0 1 2 】

V P N 識別子設定テーブルの設定単位は、物理インターフェース毎としてもよいし、下位レイヤとして同一のプロトコルが使用される複数の回線を収容するインターフェースカード単位でもよい。また、1 つの物理インターフェース内に下位レイヤとして複数のプロトコルが多重化されている場合（例えばフレームリレーと P P P が時分割多重されている回線）は、その設定単位は、物理インターフェースと I P の下位レイヤのプロトコルとの組合わせでもよい。

【 0 0 1 3 】

I S P が V P N を収容する際、I P の下位レイヤに A T M を用い、V P N 識別子として V P I、V C I を用いる場合を例に V P N エッジルータの動作を具体的に説明する。V P N エッジルータはパケットを受信すると、まず、V P N 識別子設定テーブルの設定に従い、V P N 識別子（本例の場合、V P I、V C I と設定されている）および検索すべき V P N 識別テーブルを決定する。本例の場合、V P N エッジルータは、V P I、V C I と V P N との対応が示されているテーブルを検索することになる。V P N エッジルータは、V P I、V C I を検索キーにして V P N 識別テーブルの検索を行い、受信したパケットがどの V P N に属しているかを判定する。その判定が終了すると、V P N エッジルータは、受信したパケットが属する V P N 用のルーティングテーブルを検索し、I S P ネットワーク内の次の転送先を決定し、ネットワーク内で V P N 識別のために使用されるカプセル化ヘッダ情報の生成を行う。V P N エッジルータは、パケットにヘッダ情報を付与し、決定した次の転送先へパケットを送出する。

【 0 0 1 4 】

以上の説明のように、本発明では、物理インターフェースに多重化されている論理的なチャネル番号を用いて V P N 識別を行うため、V P N エッジルータに V

PN毎に物理インターフェースを用意する必要がない。また、一つの企業ネットワークを複数のVPNと接続させたい場合、そのVPNの数だけ論理的なチャネルを用意すればよく、VPNの数だけ物理的な回線を用意する必要が無い。また、企業ネットワークからVPNサービスを行うISPネットワークまでのアクセス手段として、別のISPあるいはキャリアが提供するATM網やフレーム・リレー等を用いる場合においても、論理的なチャネルでVPN識別が行われるため、VPNを実現することができる。

【0015】

さらに、本発明によれば、ISPの管理者は、IPの下位レイヤのプロトコル毎にVPN識別子を選択し、そのVPN識別子をVPN識別子設定テーブルに設定することができるため、VPNを収容する際、下位レイヤに様々なプロトコルを用いることができる。

【0016】

【発明の実施の形態】

図1は、本発明のVPNエッジルータを用いて構成したVPNの一実施例を説明するための図である。以下では、下位レイヤとは、IPパケットをカプセル化するプロトコルを意味するものとする。また、IPパケットをIPヘッダでカプセル化する場合にも、便宜上、このカプセルヘッダを下位レイヤのヘッダとして表記することとする。

【0017】

ISPネットワーク(5)は、ネットワークのバウンダリに位置するエッジルータ(9、10)と、ネットワークコアに位置するコアルータ(17)とを有する。図1では、コアルータ(17)は一つしか示されていないが、その数はこれに限定されるものではない。ISPネットワーク(5)内部ではMPLS(ATMによる)によりカプセル化が行われVPNが実現されるものとする。上述のように、カプセル化の仕方はこれに限られない。ISPネットワーク(5)は、エッジルータ(9)を介してLAN1(1)とLAN2(2)を収容し、エッジルータ(10)を介してLAN3(3)とLAN4(4)を収容する。LAN1(1)とLAN3(3)は同一企業AのLANであり、これらのLAN間でVPN

を構成する。また、LAN 2 (2) と LAN 4 (4) は同一企業 B の LAN であり、これらの LAN 間でも VPN を構成する。企業 A、企業 B の VPN をそれぞれ VPNA (7)、VPNB (8) と呼ぶことにする。

【 0 0 1 8 】

LAN 1 と LAN 2 は、ISP ネットワーク (5) とは別の ISP またはキャリアが提供する ATM 網 (6) を介し、回線 (11) に論理的に多重化されてエッジルータ (9) に接続されている。回線 (11) とエッジルータ (9) の物理インターフェースを (12) とする。物理インターフェースとは、ルータと回線との接続点という意味である。一方、LAN 3 (3) と LAN 4 (4) はそれぞれ RFC 2615 で規定されている POS (PPP Over SONET) を用い、回線 (13)、(14) を介してエッジルータ (10) に接続されている。回線 (13)、(14) とエッジルータの物理インターフェースをそれぞれ (15)、(16) とする。

【 0 0 1 9 】

本実施例では、LAN 1 と LAN 2 が属している VPN を識別する識別子として VPI、VCI が用いられる。エッジルータ (9) 内に設けられた VPN 識別子設定テーブルにおいて、物理インターフェース (12) に対応するエントリには、VPI、VCI と設定される。エッジルータ (10) は、LAN 3 と LAN 4 が属している VPN を識別する識別子として物理インターフェースに与えられている番号を用いる。エッジルータ (10) 内に設けられた VPN 識別子設定テーブルにおいて、物理インターフェース (15)、(16) に対応するエントリには、物理インターフェースと設定される。VPN 識別子設定テーブルは後述される。

【 0 0 2 0 】

また、エッジルータ (9) 内には、VPN 識別子と、当該 VPN 識別子を有するパケットが何れの VPN に属するかを示す情報 (以下、VPN 番号という。) との対応関係を示す VPN 識別テーブルが設けられている。上記 VPNA、VPNB が VPN 番号に該当する。さらに、エッジルータ (9) 内には、宛先 IP アドレスと、出力方路及び出力パケットのカプセルヘッダ情報との関係を示すルー

ティングテーブルが設けられている。このルーティングテーブルはVPN A用のものと、VPN B用のものとが用意される。VPN 識別テーブル及びルーティングテーブルについても後述される。

【 0 0 2 1 】

エッジルータ (9) は、LAN 1 から送信されたLAN 3 宛のIP パケットを受信すると、VPN 識別子設定テーブルの設定に従い、VPN 識別子としてVPI、VCIを用いることを決定する。VPN 識別子を決定した後、エッジルータ (9) は、VPI、VCIとVPNとの対応が示されているVPN 識別テーブルを検索し、当該パケットがVPN Aに属するパケットであると判定する。次に、エッジルータ (9) は、宛先IPアドレスを検索キーとしてVPN A用のルーティングテーブルを検索し、次転送先のコアルータ (1 7) を決定し、そして、コアルータ行きのVPN Aに属するパケットのカプセルヘッダを決定する。このカプセルヘッダが付与されたパケットは、コアルータ (1 7) へ転送される。

【 0 0 2 2 】

コアルータ (1 7) は、カプセルヘッダ、すなわち、VPI、VCIと、次転送先との対応関係を示すルーティングテーブルを有しており、受信パケットのカプセルヘッダを検索キーにして次転送先 (エッジルータ (1 0)) 、および次のカプセルヘッダを決定し、前記カプセルヘッダを付与してエッジルータ (1 0) へ送信する。

【 0 0 2 3 】

エッジルータ (1 0) は、エッジルータ (9) と同様の構成であり、エッジルータ (9) と同様にして、受信パケットのカプセルヘッダを検索キーにしてVPN 識別を行い、VPN Aに属するパケットであることを判定する。次に宛先IPアドレスを検索キーとしてVPN A用のルーティングテーブルを検索して転送先を決定し、カプセルヘッダをはずしてLAN 3 へパケットを転送する。

【 0 0 2 4 】

エッジルータ (9) は、物理インターフェースに多重された論理的なチャネル番号によりVPNを識別し、当該VPNのルーティングテーブルを検索するので、一つの回線に論理的に多重されたVPNを識別することが可能となる。また、

これにより、企業Aが用いるIPアドレスと企業Bが用いるIPアドレスとがバッティングする場合でも、正しいあて先への転送が可能となる。

【0025】

VPNB内のLAN4からLAN2へパケットを送信する場合も上記の場合と同様の手続により送信が行われるが、LAN4から送信されたLAN2宛のIPパケットを受信したエッジルータ(10)は、VPN識別子として物理インターフェースを用いる点が上記の場合と異なる。

【0026】

図2は、図1に示される実施例の変形例を説明するための図である。本実施例では、LAN1とLAN2は、別回線(18)、(19)を介して、直接、ISPネットワーク(5)内の多重化装置(20)に收容される。多重化装置(20)において、VPNA、VPNBごとに異なるVPI、VCIが割り当てられる。エッジルータ(9)は、図1の場合と同様に、VPI、VCIを用いてVPN識別を行う。

【0027】

図3は、図1に示される実施例の他の変形例を説明するための図である。

【0028】

図3では、図1に示したネットワーク構成に、LAN5(21)が付け加えられており、LAN2、LAN4及びLAN5の間でVPNBが構成されている。LAN5(21)はPOSを用い、回線(22)でエッジルータ(9)に接続されている。回線(22)とエッジルータの物理インターフェースを(23)とする。

【0029】

エッジルータ(9)は、図1の説明と同様に、LAN1とLAN2が属しているVPNを識別する識別子としてVPI、VCIを用いる。一方、エッジルータ(9)は、LAN5が属しているVPNを識別する識別子として物理インターフェースを用いる。エッジルータ(9)内のVPN識別子設定テーブルには、物理インターフェース(23)に対応するエントリに物理インターフェースと設定される。本実施例では、エッジルータ(9)内に、VPI、VCIとVPNとの対

応が示されているVPN識別テーブルと、物理インターフェースとVPNとの対応が示されているVPN識別テーブルとの2種類のVPN識別テーブルが設けられている。その詳細は後述される。

【0030】

例えば、LAN5から送信されたLAN4宛のIPパケットを受信した場合、エッジルータ（9）は、VPN識別子設定テーブルの設定に従い、VPN識別子として物理インターフェースの番号を用いることを決定する。VPN識別子を決定した後、エッジルータ（9）は、物理インターフェースの番号を検索キーとして、物理インターフェースとVPNとの対応が示されているVPN識別テーブルを検索し、そのIPパケットがVPNBに属するパケットであることを判定する。次に、宛先IPアドレスを検索キーとしてVPNB用のルーティングテーブルを検索し、次転送先のコアルータ（17）を決定し、その決定したコアルータに送信されるパケットのカプセルヘッダを決定する。このカプセルヘッダをパケットに付与し、コアルータ（17）に転送する。

【0031】

本実施例では、異なる下位プロトコル毎にVPN識別子を定め、各VPN識別子対応にVPN識別テーブルを設けている。このようにすることにより、一つのルータで異なる下位プロトコルに対応する際の自由度が増す。すなわち、本実施例によれば、エッジルータに收容しようとする下位プロトコルに応じて、VPN識別子設定テーブル内のVPN識別子を設定し、そのVPN識別子に対応するVPN識別テーブルを設定しさえすれば、エッジルータにおいて様々な下位プロトコルを收容することが可能となる。

【0032】

次に、本発明のVPNエッジルータの詳細を説明する。VPNを構成する上で、ネットワークの構成は図1～図3に示したもの以外にも、多様な構成が考えられる。そこで、図1～図3のネットワークを構成する場合のVPNエッジルータの構成に限定して説明するのではなく、より一般的に、本発明VPNエッジルータの構成を説明する。

【 0 0 3 3 】

図 4 から図 8 を用いて、VPN エッジルータ (9) の一構成例を説明する。VPN エッジルータ (1 0) の構成もこれと同様である。

【 0 0 3 4 】

図 4 は、本発明の VPN エッジルータ (9) の一構成例を示す図である。制御部 (5 0) は、下位レイヤ処理部 (5 3、5 4)、パケットレイヤ処理部 (5 2) 及びスイッチ (5 1) と接続されており、VPN エッジルータ全体の制御及びルーティング処理などを行う。下位レイヤ処理部 (5 3、5 4) は、回線 (5 5、5 6) を収容するとともに、IP の下位レイヤの終端を行う。パケットレイヤ処理部 (5 2) は、下位レイヤ処理部 (5 3、5 4) から下位レイヤの情報及び IP パケットを受け取り、その下位レイヤの情報とその IP パケットのヘッダ情報とを用いてパケットの転送先を決定する。スイッチ (5 1) は複数の入出力ポートを有しており、それらのポートは、パケットレイヤ処理部と接続されている。スイッチ (5 1) は、例えば、クロスバスイッチで構成される。スイッチ (5 1) は、パケットレイヤ処理部 (5 2) からパケットを受信すると、パケットレイヤ処理部 (5 2) において決定されたパケットの転送先に対応する出力ポートに、そのパケットを出力する。前記制御部 (5 0) には制御端末 (5 7) が接続される。前記制御端末により、ルータの管理者は、ルータ内の VPN 識別子設定テーブル、VPN 識別テーブル及びルーティングテーブルの設定等を行うことが可能である。受信回線 5 5 - 1、5 5 - 2、5 5 - 3 及び 5 5 - 4 とルータ (9) との接続点には、それぞれ、物理インタフェース番号 1、2、3 及び 4 が割り当てられている。

【 0 0 3 5 】

図 5 は、パケットレイヤ処理部 (5 2) の一構成例を示す図である。下位レイヤ処理部 IF (1 0 0、1 0 6)、スイッチ IF (1 0 3、1 0 4) 及び制御部 IF (1 1 0) は、それぞれ、下位レイヤ処理部 (5 3、5 4) とのインタフェース、スイッチ (5 1) とのインタフェース及び制御部 (5 0) とのインタフェースである。本実施例の特徴の一つは、VPN 識別子設定テーブル (1 5 0)、VPN 識別テーブル (1 5 1) 及び VPN 用のルーティングテーブル (1 5 2)

を設けた点にある。これらはメモリ上に構成される。これらは、それぞれ、物理的に異なるメモリ上に構成されてもよいし、同一のメモリ上の異なる領域に構成されてもよい。この構成の仕方の差異は本発明を実施する上で本質的なものではない。VPN識別子設定テーブル（150）、VPN識別テーブル（151）、ルーティングテーブル（152）及びここで説明しなかったその他のブロックの機能・構成は、以下で説明するルータ（9）のパケット処理動作と併せて説明する。

【0036】

下位レイヤ処理部（53）が収容している回線（55）からパケットを受信し、下位レイヤ処理部（54）が収容している回線（56）へパケットを転送する場合を例に引き、ルータ（9）のパケット処理を説明する。

【0037】

下位レイヤ処理部（53）は、LANからパケットを受信すると、IPの下位レイヤのプロトコルを終端する。下位レイヤ処理部（53）は、IPパケットとともに、パケットを受信した物理インターフェース番号（以下、受信物理インターフェース番号と呼ぶ）、下位レイヤのプロトコル種別、VPN識別子として用いる下位レイヤのカプセルヘッダ情報等をパケットレイヤ処理部（52）へ転送する。

【0038】

パケットレイヤ処理部（52）内の下位レイヤ処理部インターフェース（100）は、下位レイヤ処理部（53）から転送されたIPパケット、受信物理インターフェース番号、下位レイヤのプロトコル種別及びVPN識別子として用いる下位レイヤのカプセルヘッダ情報をパケット転送処理部（101）へ転送する。パケット転送処理部（101）は、受信したIPパケットからIPヘッダ情報を抽出し、このIPヘッダ情報、受信物理インターフェース番号、下位レイヤのプロトコル種別及びVPN識別子として用いる下位レイヤのカプセルヘッダ情報をVPN識別・ルーティングテーブル検索処理部（102）へ転送する。IPパケット本体はパケット転送処理部（101）内に一時的に蓄積される。

【 0 0 3 9 】

VPN識別・ルーティングテーブル検索処理部（102）は、まず受信物理インターフェース番号、下位レイヤのプロトコル種別等を検索キーとしてVPN識別子設定テーブル（150）を検索し、VPN識別子を決定する。

【 0 0 4 0 】

図6は、VPN識別子設定テーブル（150）の一構成例を示す。各エントリは、物理インターフェース番号（200）、下位レイヤプロトコル（203）及びVPN識別子（201）とを有する。下位レイヤプロトコルがATMのエントリには、パケットの転送優先度を示すCLPのフィールドを設けてあるが、このフィールドはなくてもよい。上述の通り、エッジルータ（9）の管理者は、制御端末（57）から、VPN識別子を設定することができる。VPN識別・ルーティングテーブル検索処理部（102）は、検索キーとして受信物理インターフェース番号を用いて検索を行い、VPN識別子（201）を決定する。例えば、受信物理インターフェース番号が1の場合、VPN識別子はVPI、VCIとなり、受信物理インターフェース番号が3の場合、VPN識別子は物理インターフェース番号となる。本実施例のように、CLPフィールドを設ける場合には、VPN識別子として、VPI、VCIとCLPとの組み合わせ、物理インターフェース番号とCLPとの組み合わせを用いてもよい。VPN識別子にCLP（204）を含めた場合のメリットについては後述する。一つの物理インターフェースに対して、複数のVPNに属するパケットが論理的に多重されて送信される場合、受信物理インターフェース番号からは、そのパケットがどのVPNに属するのか判別することができない。しかし、その下位レイヤがATMの場合、VPI、VCIをVPN識別子に用いれば、そのパケットがどのVPNに属するのかを識別することが可能となる。一つの物理インターフェースに対して、一つのVPNに属するパケットしか送信されない場合には、物理インターフェース番号でVPNを識別することが可能である。検索キーとして、下位レイヤのプロトコル（203）と物理インターフェース番号（201）との組み合わせを用いてもよい。例えば、物理インターフェース番号4に接続される回線が時分割多重回線であり、前記回線に、下位レイヤのプロトコルとしてフレームリレーを用いたパケットと、PPP(Point to

o Point Protocol)プロトコルを用いたパケットが多重されているとする。また、下位レイヤプロトコルがフレームリレーのエントリに対しては、VPN識別キーとしてDLCIが設定されており、下位レイヤプロトコルがPPPのエントリに対しては、VPN識別キーとしてタイムスロット番号が設定されているとする。この場合、受信物理インタフェース番号4のみを検索キーとして検索しても、VPN識別子がDLCIであるかタイムスロット番号であるかが一意に定まらない。そこで、この場合には、受信物理インタフェース番号と下位レイヤプロトコルとの組み合わせにより、VPN識別子を検索する。

【 0 0 4 1 】

VPN識別子が決定されると、VPN識別・ルーティングテーブル検索処理部は、そのVPN識別子を検索キーとしてVPN識別テーブル(151)を検索し、受信パケットが属しているVPNを決定する。

【 0 0 4 2 】

図7(a)、(b)は、VPN識別テーブル(151)の一構成例を示す。どちらのVPN識別テーブルにおいても、各エントリは、VPN識別子(201)とVPN番号(250)とを有する。

【 0 0 4 3 】

図7(a)は、VPN識別子(201)としてVPI、VCIを用いるテーブルの例を示している。図7(a)のCLPフィールド(204)及び装置内優先度情報フィールド(251)は設けなくても良い。装置内優先度情報フィールド(251)とは、装置内におけるパケット処理の優先度情報を示すフィールドである。VPN識別・ルーティングテーブル検索処理部(102)は、検索キーとして前記のVPN識別子設定テーブルの検索により決定したVPN識別子に従い、検索キーとしてパケットヘッダ内のVPN識別情報を用いて検索を行い、VPN番号(250)を決定する。本実施例のように、VPN識別テーブル(151)にCLPフィールド(204)及び装置内優先度情報フィールド(251)を設ける場合には、検索キーとしては、パケットの転送優先度を示すCLP(204)とVPI、VCIの組み合わせを用いてもよい。CLPを検索キーに含めることにより、同一のVPN番号に属するパケットに対して、異なる装置内優先度

情報を定めることができる。例えば、” V P I、V C I = a ” かつ ” C L P = 0 ” の場合は、” 装置内優先度 = a ”、” V P I、V C I = a ” かつ ” C L P = 1 ” の場合は、” 装置内優先度 = b ” のように、同一の V P N 番号に属するパケットに対して異なる装置内優先度情報を定めることができる。

【 0 0 4 4 】

図 7 (b) は、V P N 識別子 (2 0 1) として物理インターフェース番号 (2 5 2) を用いるテーブルの例を示している。パケット処理の優先制御を行わないのであれば、図 7 (b) の装置内優先度情報フィールド (2 5 1) は設けなくても良い。

【 0 0 4 5 】

上記以外の V P N 識別子、例えば、D L C I、タイムスロット番号等が使用される場合には、図 7 (a)、(b) と同様のテーブルを構成すればよい。すなわち、V P N 識別テーブル (1 5 1) は、V P N 識別子毎に設けられ、これらの設定は、制御端末 (5 4) から設定される。V P N 識別子毎に設けられた V P N 識別テーブル (1 5 1) は、同一のメモリ上に構成されても良いし、それぞれ、異なるメモリ上に構成されてもよい。

【 0 0 4 6 】

V P N 番号が決定されると、V P N 識別・ルーティングテーブル検索処理部は、その V P N 番号に対応する V P N 用のルーティングテーブル (1 5 2) を検索し、出力方路及びその V P N 番号に属するパケットに付加される V P N 用の出力カプセルヘッダ情報を決定する。

【 0 0 4 7 】

図 8 は、V P N 用ルーティングテーブル (1 5 2) の一構成例を示す。V P N 識別・ルーティングテーブル検索処理部 (1 0 2) は、収容する V P N 毎にこの V P N 用ルーティングテーブル (1 5 2) を保持する。この V P N 毎に設けられた V P N 用ルーティングテーブル (1 5 2) は、同一のメモリ上に構成されても良いし、それぞれ異なるメモリ上に構成されてもよい。V P N 用ルーティングテーブル (1 5 2) は宛先 I P アドレス (3 0 0) と出力方路番号 (3 0 1) と出力カプセルヘッダ情報 (3 0 2) とを有する。出力方路番号 (3 0 1) は、スイ

ッチ等でパケットを所望のインターフェースに転送するための装置内識別子である。出力カプセルヘッダ情報（302）は、ISPネットワーク（5）内で用いるカプセルヘッダ情報である。VPN識別・ルーティングテーブル検索処理部（102）は、検索キーとしてIPヘッダ内の宛先IPアドレスを用いて、前記のVPN識別テーブルの検索により決定したVPN番号（250）に対応するVPN用のルーティングテーブルの検索を行い、出力方路番号（301）及び出力カプセルヘッダ情報（302）を決定する。本実施例では、VPN毎にVPN用ルーティングテーブル（152）を設けているので、複数のVPNにおいて同一のIPアドレスが使用されていても、正しい出力方路を決定することができる。

【0048】

出力方路番号（301）と出力カプセルヘッダ情報（302）とが決定されると、VPN識別・ルーティングテーブル検索処理部（102）は、その決定した出力方路（301）と出力カプセルヘッダ情報（302）とをパケット転送処理部（101）に転送する。

【0049】

パケット転送処理部（101）は、スイッチIF（103）を介して、蓄積していたIPパケット本体、出力方路番号（301）及び出力カプセルヘッダ情報（302）とをスイッチ（51）に転送する。スイッチ（51）は、パケット転送処理部（101）から受信したIPパケット本体と、その出力カプセルヘッダ情報（302）とを、その出力方路番号に対応する出力ポートに出力する。

【0050】

上記出力ポートに接続されているパケットレイヤ処理部（52）、すなわち、パケットレイヤ処理部（52）から送信されたIPパケット本体及びその出力カプセルヘッダ情報（302）を受信する側のパケットレイヤ処理部（52）は、スイッチIF（104）を介して、それらを受信する。IPパケット本体及びその出力カプセルヘッダ情報（302）を受信すると、パケット転送処理部（105）はこれらを下位レイヤ処理部IF（106）を介して下位レイヤ処理部（54）に転送する。IPパケット本体及びその出力カプセルヘッダ情報（302）を受信すると、下位レイヤ処理部（54）は、その出力カプセルヘッダ情報

に基づきカプセルヘッダを生成し、そのカプセルヘッダにより I P パケット本体をカプセル化し、そして、そのカプセル化したパケットをコアルータ (1 7) に送信する。

【 0 0 5 1 】

以上、図 4 から図 8 を用いて V P N エッジルータ装置の一構成例を説明した。本実施例のルータ装置を用いることにより、同一の物理インタフェースに、異なる V P N に属するパケットが送信される場合であっても、それらが属する V P N を識別することが可能となる。また、同一のエッジルータが、異なる I P の下位プロトコルを用いる複数の L A N を収容する場合でも、それぞれの下位プロトコルに対応した適切な V P N 識別子を V P N 識別子設定テーブルに設定することができるので、V P N 構築の自由度が増す。

【 0 0 5 2 】

本実施例では、V P N 用ルーティングテーブルの検索結果として出力カプセルヘッダ情報を直接出力しているが、出力カプセル番号を出力するようにしてもよい。この出力カプセル番号は、出力側の下位レイヤ処理部においてカプセルヘッダを付与するための装置内識別子である。この場合、出力側の下位レイヤ処理部にカプセル番号とカプセルヘッダとをペアにしたヘッダ生成テーブルを設ける。出力側の下位レイヤ処理部は、検索キーとそてカプセル番号を用いてヘッダ生成テーブルを検索し、カプセルヘッダを決定する。

【 0 0 5 3 】

本実施例で示したテーブルは論理的なテーブルであり、テーブル検索方法として、ツリー構造に代表される検索アルゴリズムを用いてもよいし、C A M (Content Addressable Memory) を使った構成や、テーブルを逐次検索していく方式を採用してもよい。

【 0 0 5 4 】

V P N エッジルータ装置が時分割多重回線を収容する場合、下位レイヤ処理部がパケットレイヤ処理部に転送する情報として、本実施例で説明した各情報の他、タイムスロット番号を加えてもよい。この場合、V P N 識別子として、V P N 識別子設定テーブルにタイムスロット番号を設定してもよい。また、V P N 識別

テーブルの検索キーとして、タイムスロット番号を用いてもよい。

【 0 0 5 5 】

V P N エッジルータ装置がイーサネットを収容し、イーサネット上のパケットがIEEE802.1Qに従ってV L A N カプセル化されている場合、下位レイヤ処理部がパケットレイヤ処理部に転送する情報として、本実施例で説明した各情報の他、V L A N T a g 情報を加えてもよい。この場合、V P N 識別子として、V P N 識別子設定テーブルにV L A N T a g 情報を設定してもよい。また、V P N 識別テーブルの検索キーとして、V L A N T a g 情報を用いてもよい。

【 0 0 5 6 】

I P パケットがL 2 T P (Layer2 Tunneling Protocol) で規定されているL 2 T P ヘッダでカプセル化されている場合、V P N 識別子として、V P N 識別子設定テーブルにL2TPカプセルヘッダ内の各情報(トンネルID、セッションID等)を設定してもよい。

【 0 0 5 7 】

また、IPパケットがPPP Over Ethernetカプセル化方式で規定されているカプセル情報でカプセル化されている場合、下位レイヤ処理部がパケットレイヤ処理部に転送する情報として、本実施例で説明した各情報の他、PPP Over Ethernetカプセル化方式で規定されているカプセル情報を加えてもよい。この場合、V P N 識別子として、V P N 識別子設定テーブルにPPP Over Ethernetカプセル化方式で規定されているカプセル情報(セッションID等)を設定してもよい。

【 0 0 5 8 】

図9は、本発明のV P N エッジルータ装置(9)の他の構成例を示す。インターフェースカード(400、401)は、それぞれ、同一の下位レイヤのプロトコルを用いる回線を収容するカードである。例えばインターフェースカード(400)はA T M 用のインターフェースカードであり、A T M 回線(402)を収容する。また、インターフェースカード(401)はP O S 用のインターフェースカードであり、P O S 回線(403)を収容する。インターフェースカード(400、401)は着脱可能であり、ルータの管理者は、必要な下位レイヤプロトコル用のインターフェースカードを必要な数量だけ搭載することができる。各

インターフェースカードには、各下位レイヤプロトコルに特有の処理を行う下位レイヤ処理部（４０５、４０６）が搭載されている。下位レイヤ処理部（４０５、４０６）の動作は、図４の下位レイヤ処理部（５３、５４）と同様である。パケット処理カード（４０７）は前記インターフェースカードからＩＰパケット等の情報を受け取り、パケットレイヤ処理を行うカードである。各パケット処理カード（４０７）は着脱可能であり、ルータの管理者は、必要な数量だけ搭載することができる。各パケット処理カード（４０７）には、図４、図５を用いて説明したパケットレイヤ処理部（５２）が搭載されている。管理者は、収容するインターフェースカードの種別、ＬＡＮとインターフェースカードとの間のアクセス網の構成に応じて、制御端末（５７）から、パケット処理カード（４０７）内のＶＰＮ識別子設定テーブル、ＶＰＮ識別テーブル、ＶＰＮ用ルーティングテーブルの構成をフレキシブルに設定することができる。本実施例のＶＰＮエッジルータ装置のパケット処理動作は、図４から図８を用いて説明した動作と同様である。

【 0 0 5 9 】

図１０から図１２は、図９のパケット処理カード（４０７）に収容されるインターフェースカードと、パケット処理カードに保持されるＶＰＮ識別子設定テーブル、ＶＰＮ識別テーブル、ＶＰＮ用ルーティングテーブルとの関係を示す図である。図１０から図１２は、エッジルータに収容されるＬＡＮと、エッジルータ（９）の構成要素のうちインターフェースカードとパケット処理カードのみを示す。また、パケット処理カード内のＶＰＮ識別子設定テーブル、ＶＰＮ識別テーブル、ＶＰＮ用ルーティングテーブルは論理的なものである。図１０から図１２では、同一インターフェースカード内の全物理インターフェースに対し、同じＶＰＮ識別子が使用される場合を示している。このため、ＶＰＮ識別子設定テーブルの検索キーとして物理インターフェース番号を設定する必要がないので、図１０から図１２では、その検索キーとしての物理インターフェース番号は省略されている。同一インターフェースカード内で、異なるＶＰＮ識別子が使用される場合は、上述のようにＶＰＮ識別子設定テーブルの検索キーとして物理インターフェースを用いればよい。

【 0 0 6 0 】

図 1 0 は、パケット処理カード (4 0 7) に A T M 用インターフェースカード (4 0 0) が収容される場合における、パケット処理カード内の V P N 識別子設定テーブル、V P N 識別テーブル、V P N 用ルーティングテーブルの一構成例を示す。L A N 1 (4 5 0) は V P N A に属し、L A N 2 (4 5 1) は V P N B に属しているとする。L A N 1、L A N 2 からのパケットは多重化装置 (4 5 2) で多重され、回線 (4 5 3) を介して A T M 用インターフェースカード (4 0 0) に収容される。多重される際、L A N 1、L A N 2 からのパケットには V P I、V C I としてそれぞれ a、b という値が割り当てられているとする。本実施例では、V P N 識別には V P I、V C I を用いる。パケット処理カード (4 0 7) 内の V P N 識別子設定テーブル (4 5 5) には V P N 識別子として V P I、V C I が設定される。V P N 識別テーブル (4 5 6) には検索キーとして V P I、V C I が設定される。V P N 用ルーティングテーブルとしては V P N A 用ルーティングテーブル (4 5 7)、V P N B 用ルーティングテーブル (4 5 8) が設けられる。例えば、L A N 1 からパケットを受信すると、A T M 用インターフェースカード (4 0 0) 内の下位レイヤ処理部 (4 0 5) は、A T M プロトコルを終端し、I P パケット本体及び V P I、V C I、物理インターフェース番号等をパケット処理カード (4 0 7) に転送する。パケット処理カード (4 0 7) 内の V P N 識別・ルーティングテーブル検索処理部は、V P N 識別子設定テーブル (4 5 5) を検索し、V P N 識別子として V P I、V C I を用いることを決定する。次に、受信パケットの V P I、V C I の値、" a "、を用いて V P N 識別テーブル (4 5 6) を検索し、受信パケットが V P N A に属することを判定する。次に V P N A 用のルーティングテーブル (4 5 7) を検索し、出力方路、および出力カプセルヘッダ情報を決定する。

【 0 0 6 1 】

図 1 1 は、パケット処理カード (4 0 7) に P O S 用インターフェースカード (4 0 1) が収容される場合における、パケット処理カード内の V P N 識別子設定テーブル、V P N 識別テーブル、V P N 用ルーティングテーブルの一構成例を示す。

【 0 0 6 2 】

LAN 1 (4 5 0) は VPNA に属し、LAN 2 (4 5 1) は VPNB に属しているとする。LAN 1、LAN 2 はそれぞれ回線 (5 0 0)、(5 0 1) を介して POS 用インターフェースカード (4 0 1) に収容される。回線 (5 0 0) 及び回線 (5 0 1) と POS 用インターフェースカード (4 0 1) との物理インターフェース番号をそれぞれ 1、2 とする。この場合、VPN 識別には物理インターフェースを用いるため、パケット処理カード (4 0 7) 内の VPN 識別子設定テーブル (4 5 5) には VPN 識別子として物理インターフェース番号が設定される。VPN 識別テーブル (4 5 6) には検索キーとして物理インターフェース番号を設定する。VPN 用ルーティングテーブルとして、VPNA 用ルーティングテーブル (4 5 7)、VPNB 用ルーティングテーブル (4 5 8) が設けられる。パケット処理カード (4 0 7) 内の処理は、図 1 0 を用いて説明した処理と同様である。ただし、VPN 識別子として VPI、VCI ではなく、物理インターフェースを用いる点が異なる。

【 0 0 6 3 】

図 1 2 は、図 9 に図示していないが、パケット処理カード (4 0 7) に時分割多重回線用のインターフェースカード (5 5 0) が収容される場合における、パケット処理カード内の VPN 識別子設定テーブル、VPN 識別テーブル、VPN 用ルーティングテーブルの一構成例を示す。LAN 1 (4 5 0)、LAN 2 (4 5 1)、LAN 3 (5 5 1) LAN 4 (5 5 2) はそれぞれ VPNA、VPNB、VPNC、VPND に属しているとする。LAN 1、LAN 2 の下位プロトコルはフレームリレーとし、LAN 3、LAN 4 の下位プロトコルは PPP (Point to Point Protocol) とする。LAN 1 と LAN 2 からのパケットには DLCI としてそれぞれ 1 0、2 0 が割り当てられ、それらのパケットは、フレームリレー多重化装置 (5 5 3) において、回線 (5 5 4) に多重化される。さらに、時分割多重化装置 (5 5 5) において、回線 (5 5 4)、(5 5 6)、(5 5 7) が回線 (5 5 8) に多重される。この際、回線 (5 5 4)、(5 5 6)、(5 5 7) のデータにはそれぞれ、タイムスロット番号 1、2、3 が割り当てられるとする。LAN 1、LAN 2 に対する VPN 識別子としては DLCI が用いられ

、LAN 3、LAN 4 に対するVPN識別子としてはタイムスロット番号が用いられるとする。この場合、VPN識別子設定テーブル(455)における、下位レイヤプロトコル(559)がフレームリレーであるエントリに対しては、VPN識別子としてDLCI(560)が設定される。また、下位レイヤがPPPであるエントリに対してはVPN識別子としてタイムスロット番号(561)が設定される。VPN識別テーブルとして、2つのテーブル、すなわち、DLCIとVPN番号の対応を示すVPN識別テーブル(562)と、タイムスロット番号とVPN番号の対応を示すVPN識別テーブル(563)とが設けられる。また、VPN用ルーティングテーブルとして、VPNA用ルーティングテーブル(457)、VPNB用ルーティングテーブル(458)、VPNC用ルーティングテーブル(564)及びVPND用ルーティングテーブル(565)が設けられる。パケット処理カード(407)内の処理は、図10を用いて説明した処理と同様である。ただし、VPN識別子設定テーブル検索時に、検索キーとして下位レイヤプロトコル(559)を用いる点が異なる。またVPN識別子設定テーブル検索の結果、VPN識別子として、LAN 1、LAN 2 から受信したパケットに関してはDLCIが使用され、LAN 3、LAN 4 から受信したパケットに関してはタイムスロット番号が使用される点が異なる。

【0064】

図9から図12では、1つのパケット処理カードが1つのインターフェースカードを収容する例について説明したが、パケット処理カードが複数のインターフェースカードを収容する構成をとってもよい。その際、収容する複数のインターフェースカードが異なる下位プロトコル用のものであってもよい。

【0065】

図13は、パケット処理カード(407)に異なる下位プロトコル用のインターフェースカードが収容される場合における、パケット処理カード内のVPN識別子設定テーブル、VPN識別テーブル、VPN用ルーティングテーブルの一構成例を示す。インターフェースカード(400)、(401)はそれぞれATM用、POS用とする。図13は、同一インターフェースカード内の全物理インターフェースに対し、VPN識別子が同じ場合を示している。本実施例で、パケッ

ト転送カードは複数のインターフェースカードを収容するため、各インターフェースカード（４００）、（４０１）にはそれぞれカード番号１、２が割り当てられている。また、VPN識別子設定テーブル（４５５）の検索キーとして、カード番号（６０２）が設定される。LAN１（４５０）、LAN２（４５１）、LAN３（５５１）LAN４（５５２）はそれぞれVPNA、VPNB、VPNC、VPNDに属しているとする。LAN１、LAN２からのパケットは多重化装置（４５２）で多重され、回線（４５３）を介してATM用インターフェースカード（４００）に収容される。多重される際、LAN１、LAN２からのパケットにはVPI、VCIとしてそれぞれa、bという値が割り当てられるものとする。この場合、VPN識別にはVPI、VCIを用いればよい。VPN識別子設定テーブル（４５５）における、カード番号１のエントリ（６０３）に対しては、VPN識別子としてVPI、VCIが設定される。LAN３、LAN４はそれぞれ回線（５００）、（５０１）を介してPOS用インターフェースカード（４０１）に収容される。回線（５００）、（５０１）とPOS用インターフェースカード（４０１）との物理インターフェース番号をそれぞれ１、２とする。この場合、VPN識別には物理インターフェースを用いればよい。VPN識別子設定テーブル（４５５）における、カード番号２のエントリ（６０４）に対しては、VPN識別子として物理インターフェースが設定される。VPN識別テーブルとしては、VPI、VCIとVPN番号の対応を示すテーブル（６００）と、物理インターフェース番号とVPN番号の対応を示すテーブル（６０１）とが設けられる。VPN用ルーティングテーブルとしてはVPNA用ルーティングテーブル（４５７）、VPNB用ルーティングテーブル（４５８）、VPNC用ルーティングテーブル（５６４）、VPND用ルーティングテーブル（５６５）とが設けられる。パケット処理カード（４０７）内の処理は、図１０を用いて説明した処理と同様である。ただし、VPN識別子設定テーブル検索時に、検索キーとしてカード番号（６０２）を用いる点が異なる。ここでは、ATMとPOSとを収容する場合を示したが、この組み合わせに限られるものではない。例えば、POS用インタフェースカードをFR用インタフェースカードに換えることも可能である。この場合、LAN３及びLAN４からのパケットは、LAN１及びLAN

2と同様に、一本の回線に多重してFR用インタフェースカードに入力されるように、DLCIでVPNを識別するようにしてもよい。

【0066】

以上、図9から図13を用いて説明したように、本実施例のルータ装置によれば、管理者は、収容するインタフェースカードの種別に応じて、制御端末（57）から、パケット処理カード（407）内のVPN識別子設定テーブル、VPN識別テーブル、VPN用ルーティングテーブルの構成をフレキシブルに設定することができる。また、物理インターフェースに多重された論理的なチャンネル番号によりVPNを識別するので、一つの回線に論理的に多重されたVPNを識別することが可能となる。

【0067】

図14に、インタフェースカードを装着する際の、パケット処理カード（407）の設定手順の一例を示す。VPNエッジルータ（9）にインタフェースカードが装着された後、パケット処理カード（407）内のVPN識別子設定テーブル（455）が設定される（701、702）。VPN識別子設定テーブルの設定は、装着するインタフェースカードの種別により、管理者が自由に設定することができる。次に、設定されたVPN識別子毎に、VPN識別テーブルが設定される（703）。VPN毎にルーティングテーブルが設定される（704）。

【0068】

VPN識別子の設定は、インターフェースカードをパケット処理カードに装着する際に、インターフェースカードとパケット処理カード間で通信を行い、インターフェースカードが終端するIPパケットの下位レイヤのプロトコルを自動的に判定してパケット処理カードに通知するようにしてもよい。その通知された下位レイヤのプロトコルに対応して規定された識別情報を、VPN識別子設定テーブルに自動設定することができる。

【0069】

以上、図1～図14を用いて本発明のVPNエッジルータの動作を説明した。これらに共通する動作フローを図15に示す。

【0070】

VPNエッジルータは、LANからIPパケットをカプセル化したパケットを受信すると(801)、VPN識別子設定テーブルを検索し(802)、受信パケットのVPN識別子を決定する(803)。VPN識別子としては、VPI、VCI等、論理的なチャネル識別子を用いるが、収容する下位プロトコルに応じて、これと物理インタフェース番号等とを組み合わせ使用してもよい。次に、決定したVPN識別子を検索キーとして、VPN識別テーブルを検索し(804)、受信パケットが属するVPNを決定する(805)。例えば、VPN識別子がVPI、VCIである場合には、受信パケットに割り当てられたVPI、VCIを検索キーとして、VPN識別テーブルを検索し、受信パケットが属するVPNを決定する。決定されたVPN用のルーティングテーブルを検索し(806)、出力方路および出力用カプセルヘッダを決定する(807)。

【0071】

【発明の効果】

本発明のルータを用いることにより、物理インターフェースに多重化されている論理的なチャネル番号を用いてVPNを識別することができる。従って、物理回線を増やすことなく、収容するVPNの数を増やすことができる。

【0072】

また、ルータが収容する複数のLANがそれぞれ異なるIPの下位プロトコルを用いる場合でも、それぞれのプロトコルに対応した適切なVPN識別子を設定することができるので、VPN識別を行うことができる。

【図面の簡単な説明】

【図1】

本発明のVPNエッジルータを用いて構成したVPNの一実施例を説明するための図である。

【図2】

図1に示される実施例の変形例を説明するための図である。

【図3】

図1に示される実施例の他の変形例を説明するための図である。

【図 4】

本発明の V P N エッジルータの一構成例を示す図である。

【図 5】

パケットレイヤ処理部の一構成例を示す図である。

【図 6】

V P N 識別子設定テーブル（1 5 0）の一構成例を示す図である。

【図 7】

V P N 識別テーブルの一構成例を示す図である。

【図 8】

V P N 用ルーティングテーブルの一構成例を示す図である。

【図 9】

本発明の V P N エッジルータ装置の他の構成例を示す図である。

【図 1 0】

パケット処理カードに A T M 用インターフェースカードが收容される場合における、パケット処理カード内の V P N 識別子設定テーブル、V P N 識別テーブル、V P N 用ルーティングテーブルの一構成例を示す図である。

【図 1 1】

パケット処理カードに P O S 用インターフェースカードが收容される場合における、パケット処理カード内の V P N 識別子設定テーブル、V P N 識別テーブル、V P N 用ルーティングテーブルの一構成例を示す図である。

【図 1 2】

パケット処理カードに時分割多重回線用のインターフェースカードが收容される場合における、パケット処理カード内の V P N 識別子設定テーブル、V P N 識別テーブル、V P N 用ルーティングテーブルの一構成例を示す図である。

【図 1 3】

パケット処理カードに異なる下位プロトコル用のインターフェースカードが收容される場合における、パケット処理カード内の V P N 識別子設定テーブル、V P N 識別テーブル、V P N 用ルーティングテーブルの一構成例を示す図である。

【図 1 4】

パケット処理カードの設定手順の一例を示す図である。

【図 1 5】

本発明のVPNエッジルータの動作フローを示すフローチャートである。

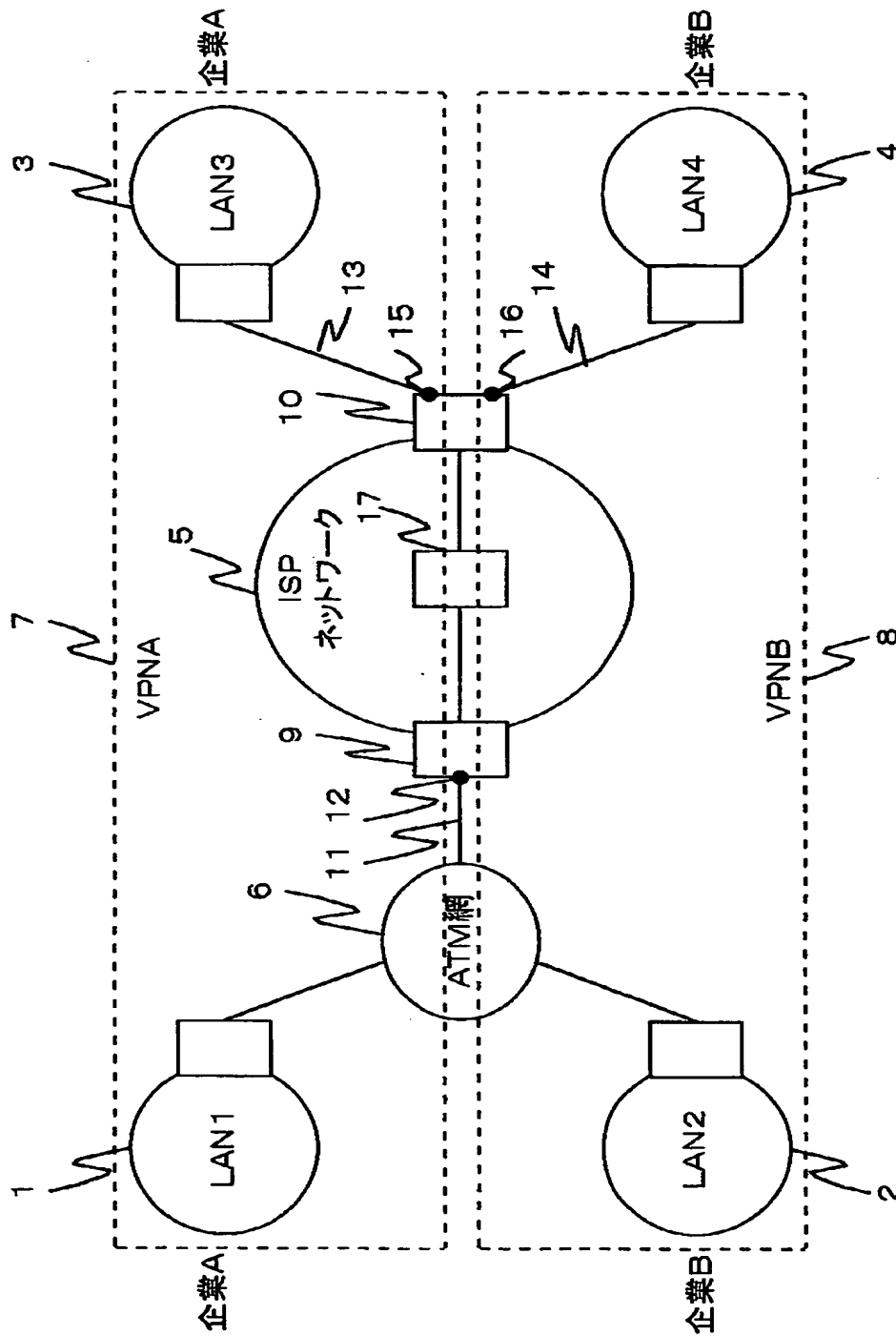
【符号の説明】

5…ISPネットワーク、9…VPNエッジルータ、50…制御部、51…スイッチ、52…パケットレイヤ処理部、53、54…下位レイヤ処理部、101、105…パケット転送処理部、102…VPN識別・ルーティングテーブル検索処理部、150…VPN識別子設定テーブル、151…VPN識別テーブル、152…ルーティングテーブル、400…ATM用インターフェースカード、401…POS用インターフェースカード、407…パケット処理カード。

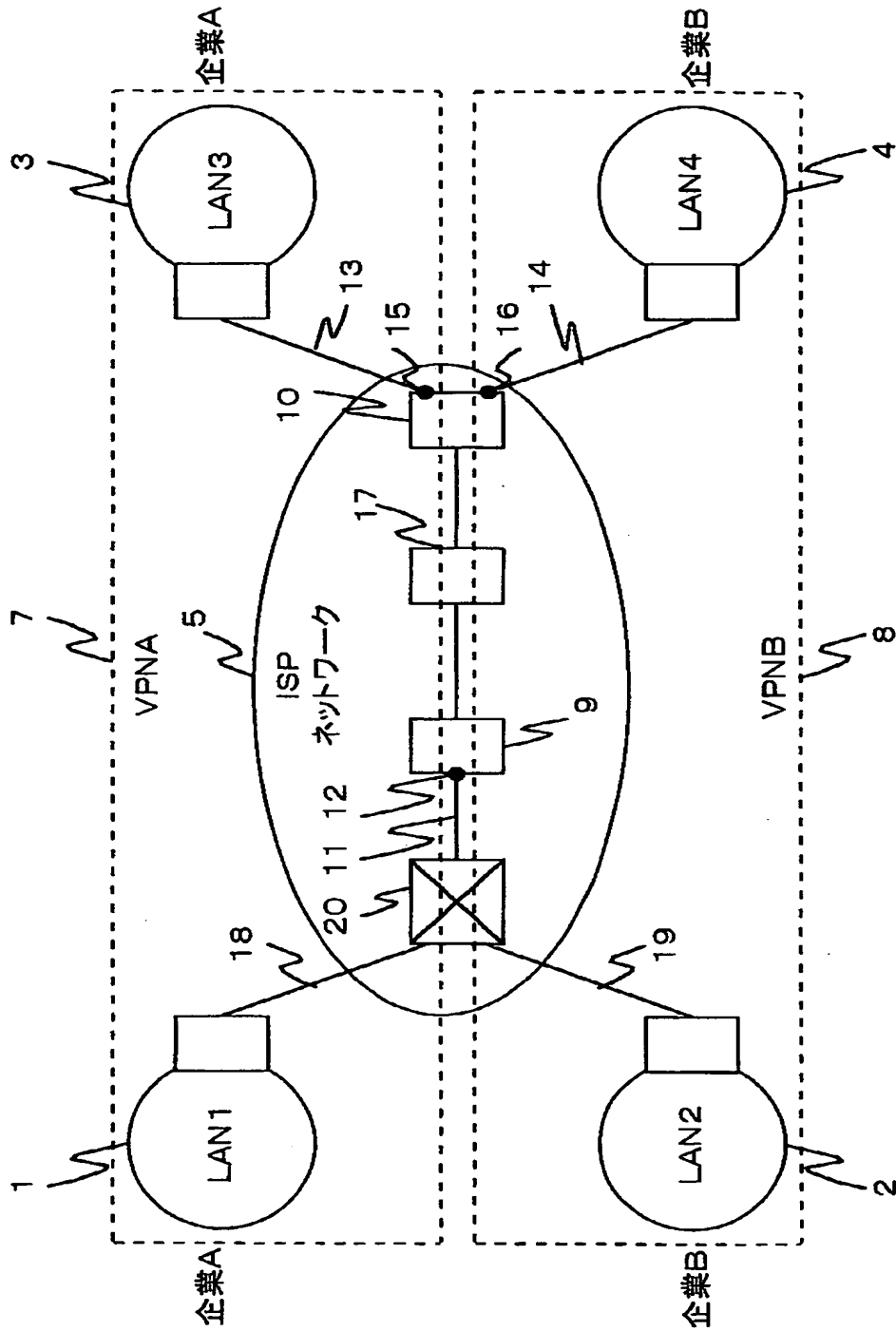
【書類名】図面

【図1】

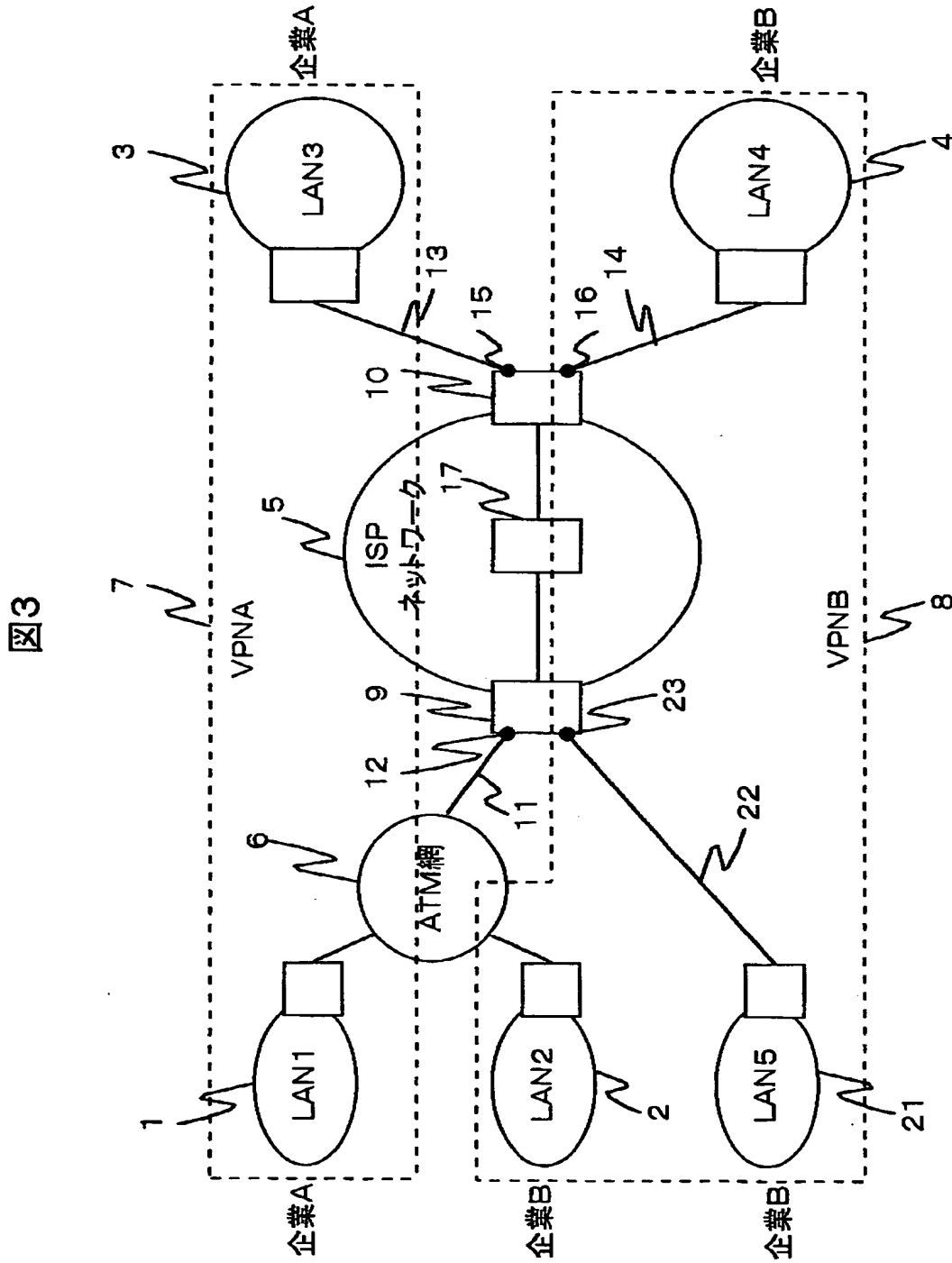
図1



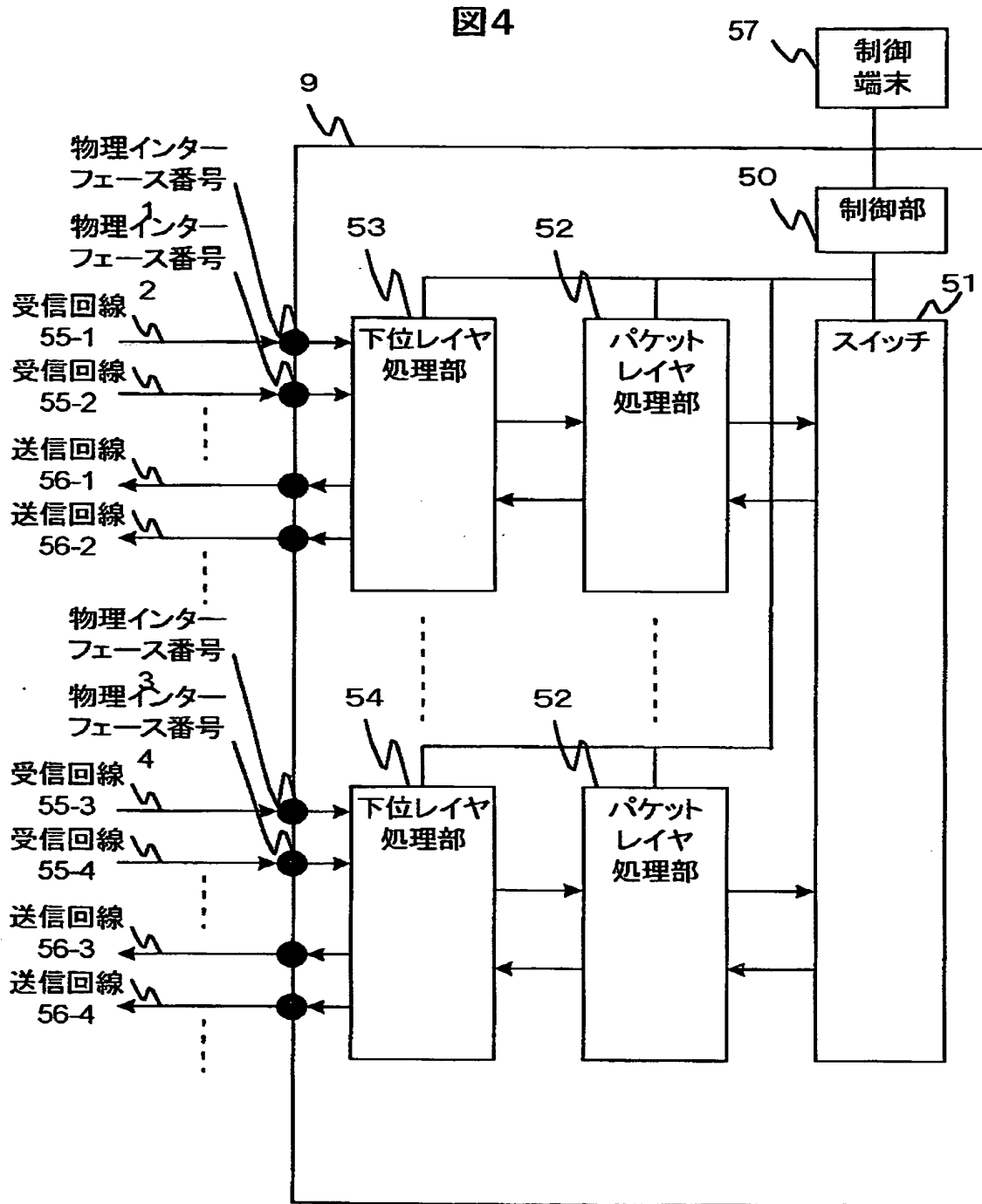
【図2】



【図3】

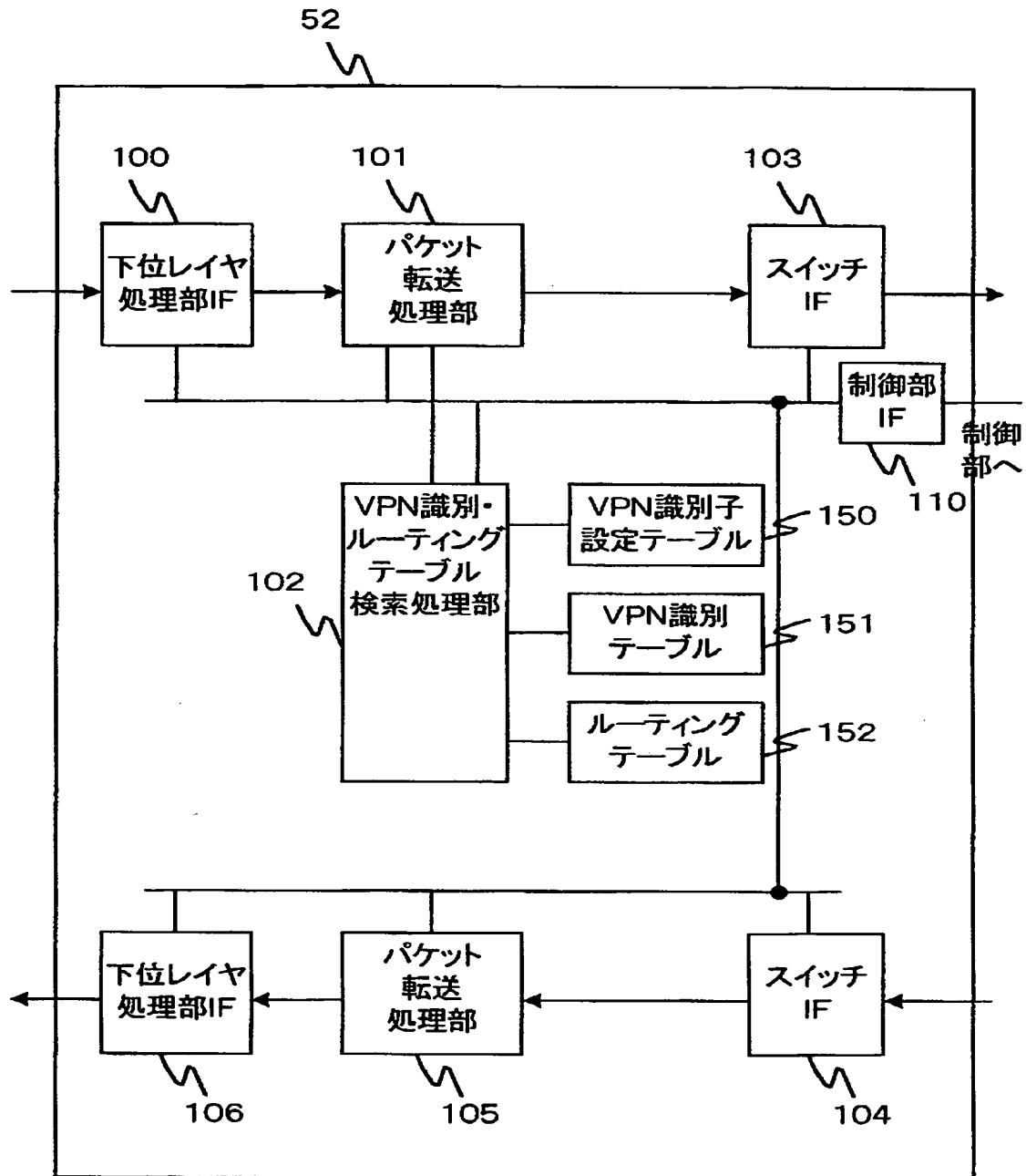


【図4】



【図5】

図5



【図 6】

図6

200 物理インターフェース 番号	203 下位レイヤの プロトコル	202 VPN識別子	201 VPI, VCI	204 CLP
1	ATM	VPI, VCI		CLP
2	ATM	VPI, VCI		CLP
3	ATM	物理インターフェース番号		CLP
4	FR	DLCI		
4	PPP	タイムスロット番号		
⋮	⋮	⋮		

← 検索キー 検索結果 →

【図 7】

図 7
(a)

VPN識別子		VPN番号	
VPI, VCI	CLP	VPN番号	装置内優先度情報
a	0	VPNA	a
a	1	VPNA	b
b	0	VPNB	c
b	1	VPNB	d
⋮	⋮	⋮	⋮

検索キー 検索結果

(b)

VPN識別子	VPN番号	
物理インターフェース番号	VPN番号	装置内優先度情報
3	VPNA	a
⋮	⋮	⋮
n	VPNB	b
⋮	⋮	⋮

検索キー 検索結果

【図 8】

図 8

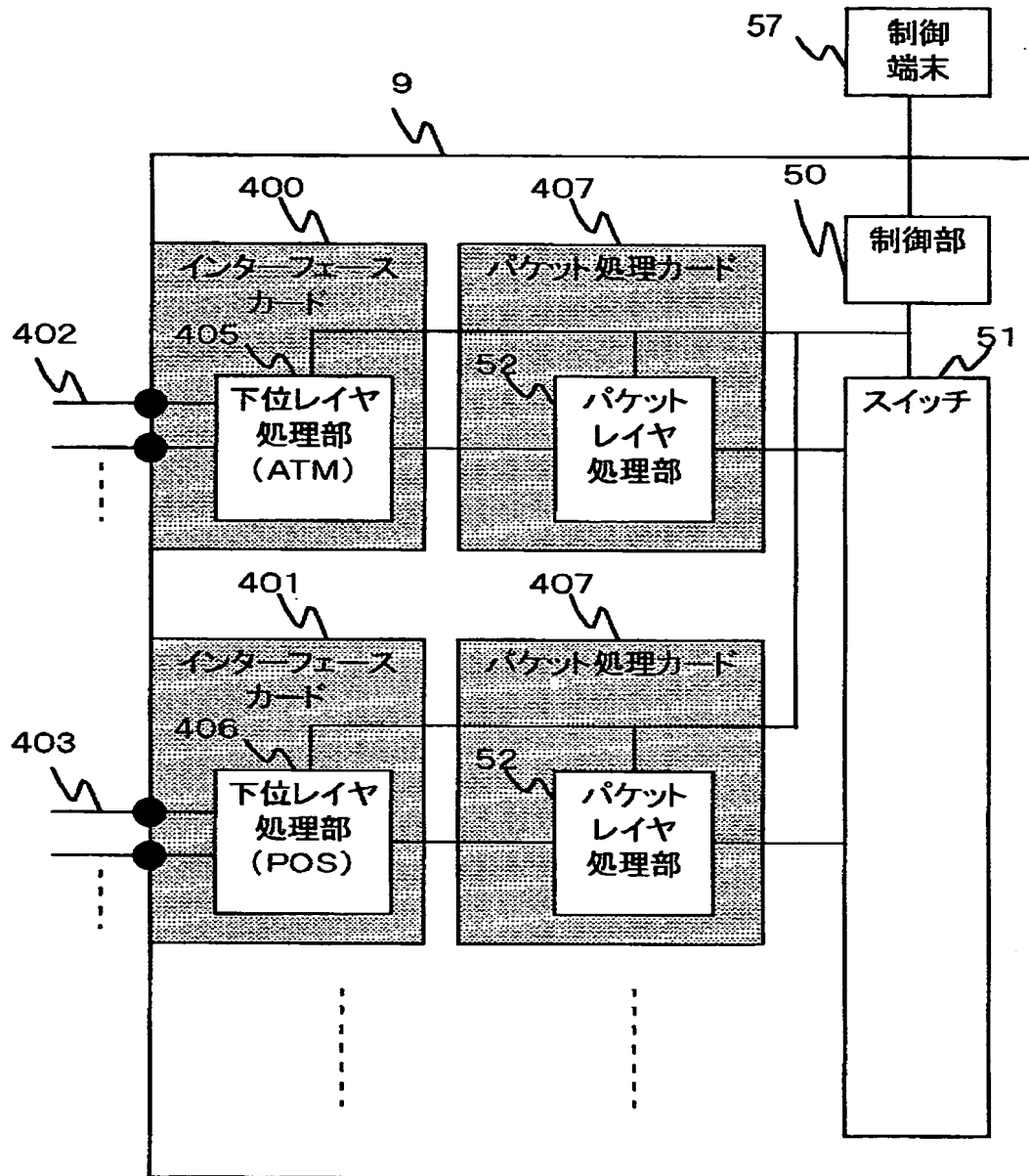
宛先IPアドレス	出力方路番号	出力カプセルヘッダ情報
a. a. a. a	10	a
b. b. b. b	11	b
⋮	⋮	⋮
n. n. n. n	15	n

検索キー

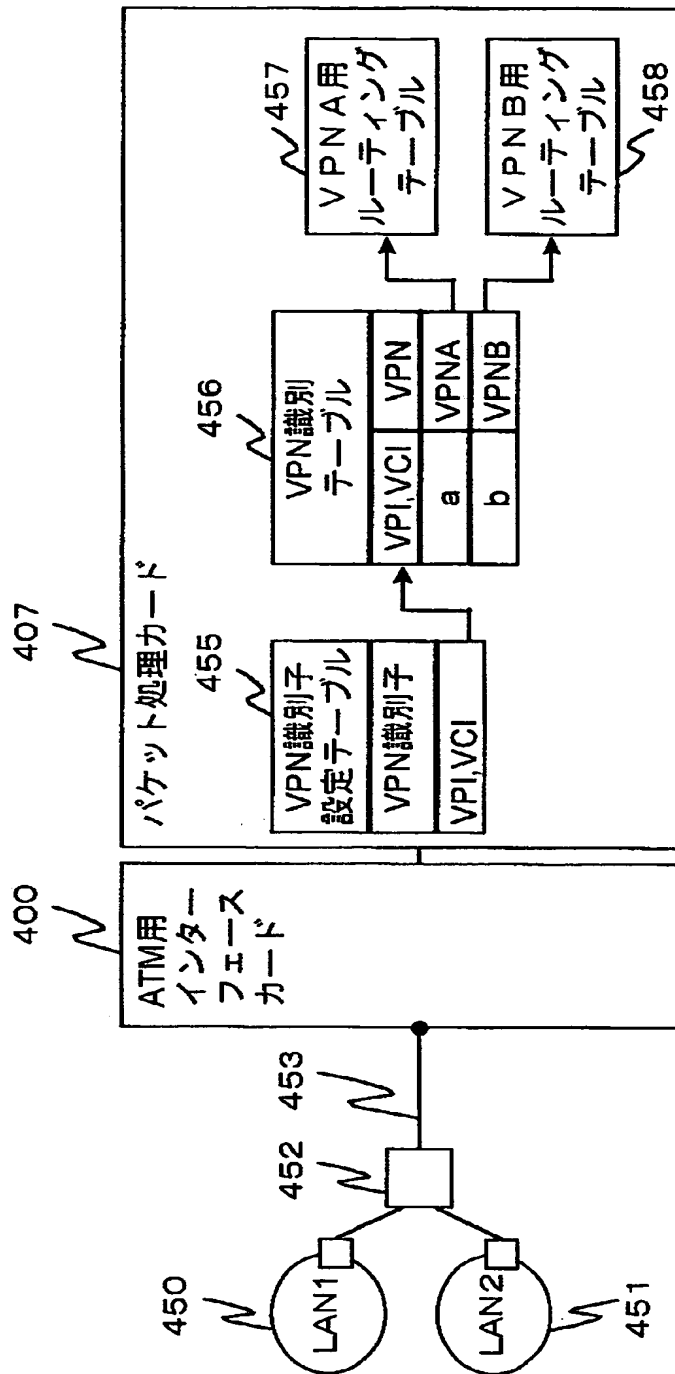
検索結果

【図9】

図9

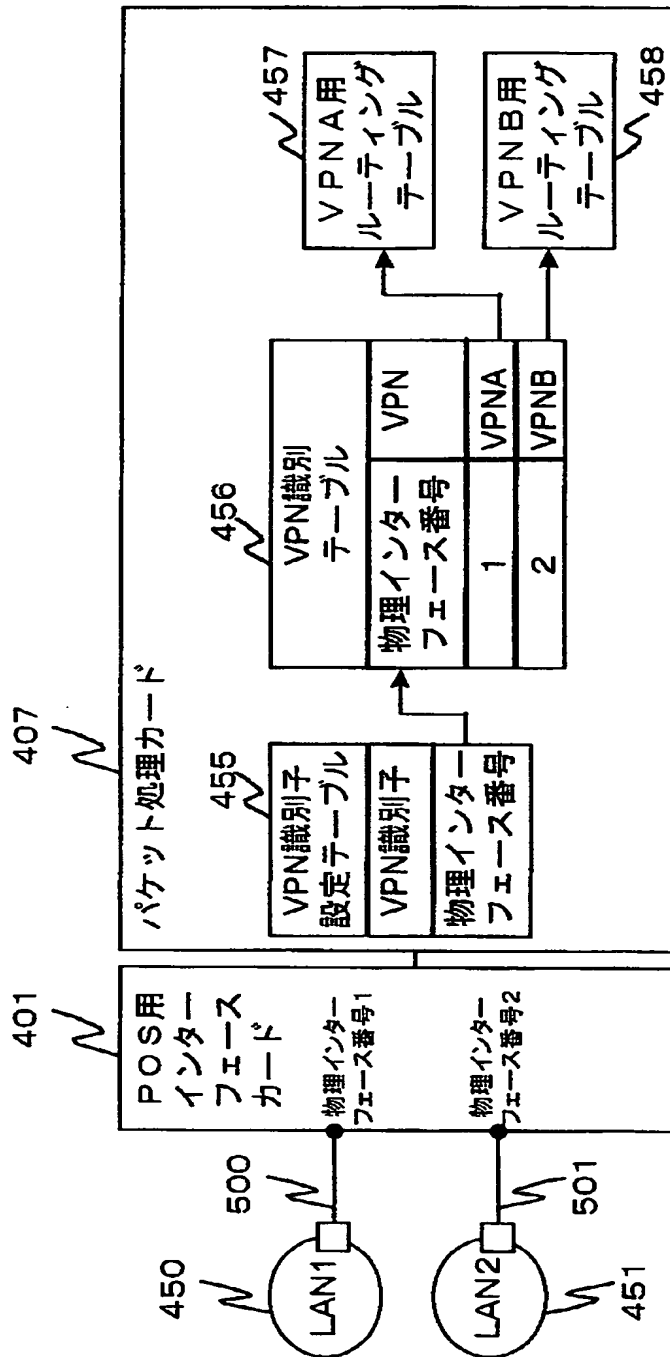


【図10】



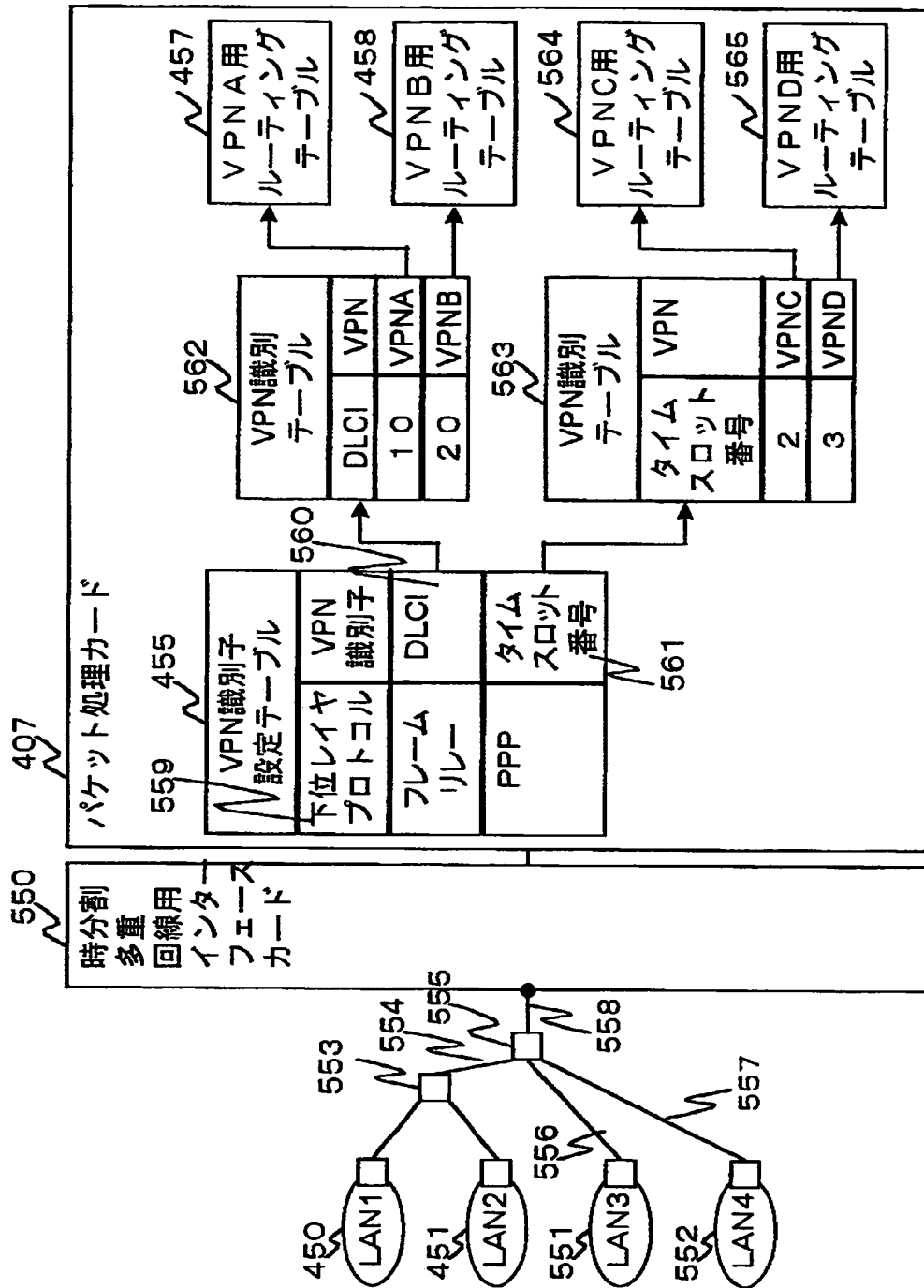
【図11】

図11



【図12】

図12



【図13】

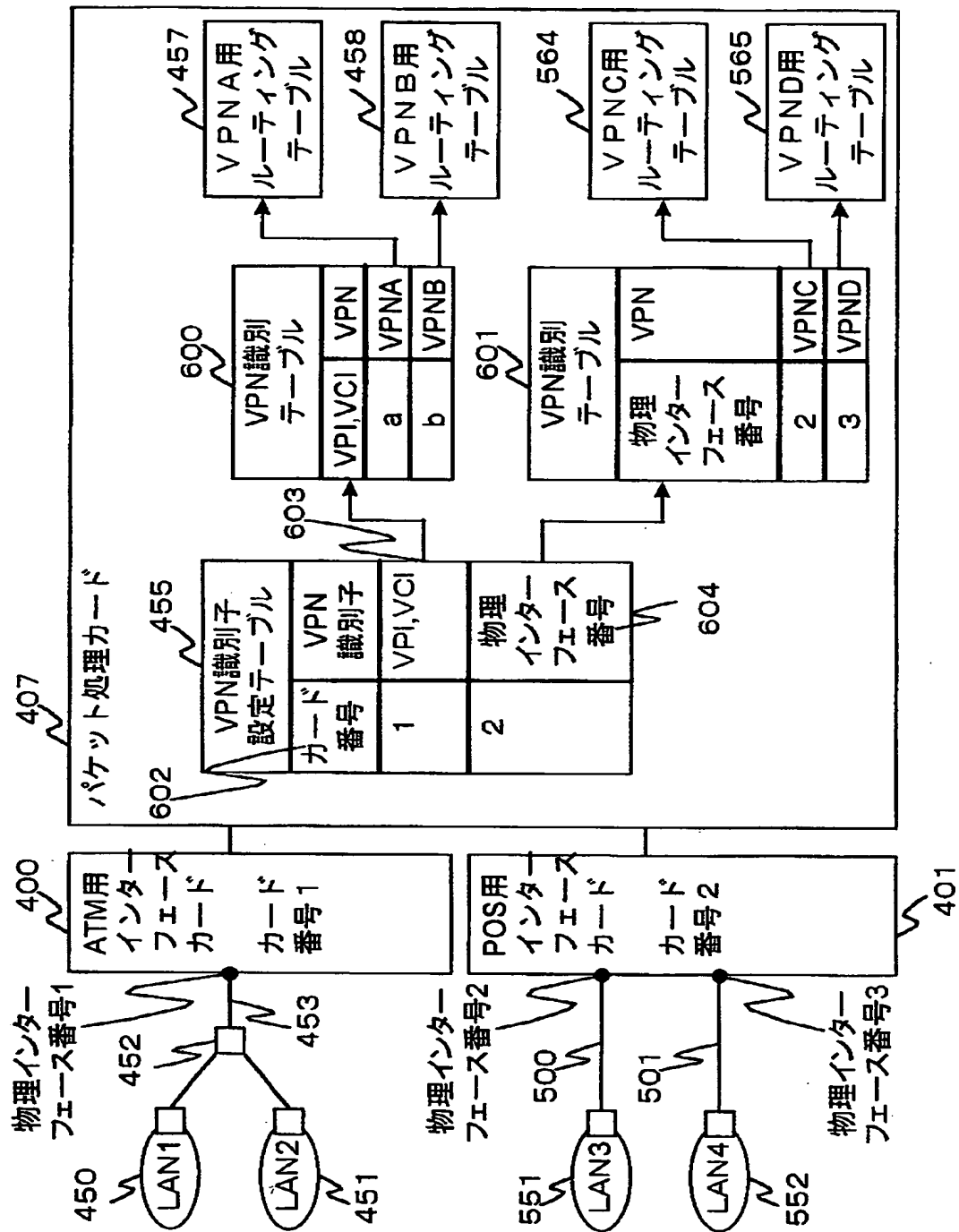
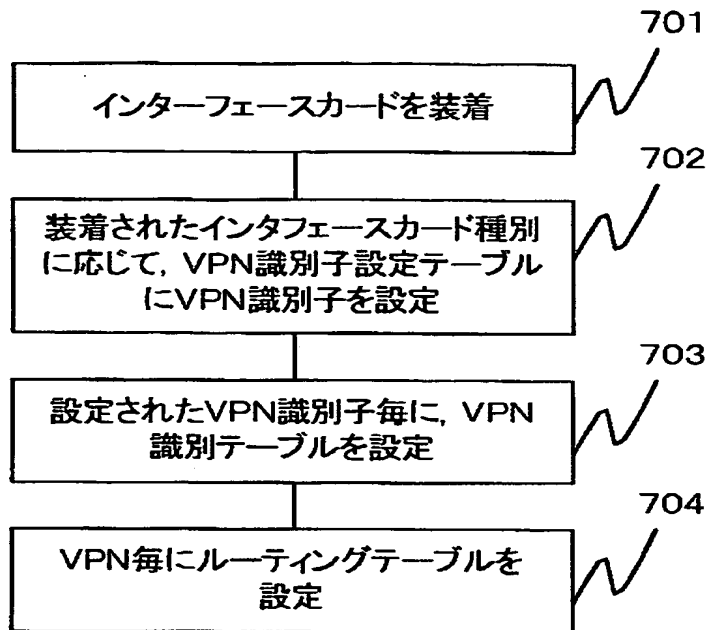


図13

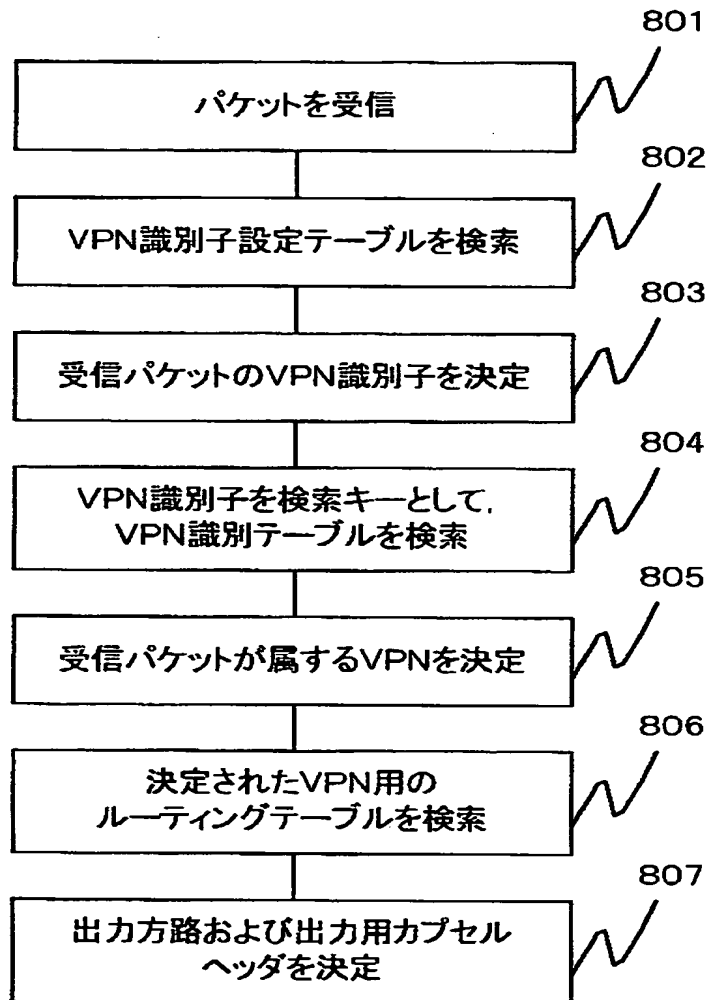
【図14】

図14



【図15】

図15



【書類名】 要約書

【要約】

【課題】 同一回線に複数のVPN (Virtual Private Network) が多重される場合に、この回線を収容するエッジルータにおいて、受信したパケットが何れのVPNに属するかを識別する手段を提供することである。

【解決手段】 VPNエッジルータに、同一回線に多重化されている論理的なチャンネル番号を用いてVPNを識別する機能を設ける。

【効果】 物理インターフェースに多重化されている論理的なチャンネル番号を用いてVPNを識別することができる。従って、物理回線を増やすことなく、収容するVPNの数を増やすことができる。

【選択図】 図 5

出 願 人 履 歴 情 報

識別番号 [0 0 0 0 0 5 1 0 8]

1. 変更年月日 1 9 9 0 年 8 月 3 1 日

[変更理由] 新規登録

住 所 東京都千代田区神田駿河台4丁目6番地

氏 名 株式会社日立製作所